UNIVERSIDAD ANDINA SIMÓN BOLIVAR

SEDE ECUADOR

PROGRAMA DE MAESTRÍA EN FINANZAS Y GESTIÓN DEL RIESGO

TÍTULO:

"METODOLOGÍA PARA EL DESARROLLO DEL PLAN DE CONTINUIDAD DE RIESGO OPERATIVO DEL BANCO ECUATORIANO DE LA VIVIENDA (BEV)"

AUTOR:

ING. MARÍA ELENA OCHOA VÁSQUEZ

2011

Al presentar esta tesis como uno de los requisitos previos para la obtención del grado de magíster de la Universidad Andina Simón Bolívar, autorizo al centro de información o a la biblioteca de la universidad para que haga de esta tesis un documento disponible para su lectura según las normas de la universidad.

Estoy de acuerdo en que se realice cualquier copia de esta tesis dentro de las regulaciones de la universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial.

Sin perjuicio de ejercer mi derecho de autor, autorizo a la Universidad Andina Simón Bolívar la publicación de esta tesis, o de parte de ella, por una sola vez dentro de los treinta meses después de su aprobación.

ING. MARÍA ELENA OCHOA VÁSQUEZ

14 de octubre del 2011

UNIVERSIDAD ANDINA SIMÓN BOLIVAR

SEDE ECUADOR

PROGRAMA DE MAESTRÍA EN FINANZAS Y GESTIÓN DEL RIESGO

TÍTULO:

METODOLOGÍA PARA EL DESARROLLO DEL PLAN DE CONTINUIDAD DE RIESGO OPERATIVO DEL BANCO ECUATORIANO DE LA VIVIENDA (BEV)"

AUTOR:

ING. MARÍA ELENA OCHOA VÁSQUEZ

TUTOR:

ING. MARIO JARAMILLO

QUITO, OCTUBRE 2011

ABSTRACT

El Banco Ecuatoriano de la Vivienda (BEV) constituye una de las principales herramientas que dispone el Estado Ecuatoriano para el desarrollo de sus políticas sociales, desde su creación la gestión del BEV estuvo dirigida a la solución del déficit habitacional en el Ecuador, debido a que es una institución financiera publica y al estar enfrentada a eventos de riesgo que podrían ocasionar la suspensión de sus actividades es necesario mantenga vigentes sus políticas de gestión de riesgos enmarcados dentro de la continuidad de negocios.

La Superintendencia de Bancos y Seguros dispuso a través de la Resolución No. 834 de Riesgo Operativo, que las instituciones del sistema financiero implementen planes de continuidad de negocios a fin de garantizar su trabajo en forma permanente y así minimizar las perdidas en casos de interrupción de sus operaciones.

El presente trabajo de investigación está enfocado en la aplicación de las mejores prácticas de riesgo operativo y de continuidad de los negocios para la elaboración de una metodología que permita al BEV contar con lineamientos para la estructuración de los planes de contingencia y continuidad de los negocios, que le faculten a la institución el establecer su cadena de valor y sus procesos críticos sobre los cuales deberá desarrollar sus planes de acción. Adicionalmente, se pretende concientizar al Gobierno Corporativo del BEV sobre la importancia de contar con planes de continuidad, para proteger la imagen de la organización y así enfrentar los riesgos que puedan ocasionar la suspensión de sus actividades.

I N D I C E

I N D I C E D E T A B L A S

I N D I C E D E G R Á F I C O S

1. PLANTEAMIENTO DEL PROBLEMA

1.1.- ANTECEDENTES

En el documento "Gestión de Riesgos Corporativos, Marco Integrado" -elaborado por el *Comitee of Sponsoring Organizations of the Treadway Comisión* (COSO)- se establece la importancia del control interno dentro de la organización y recomienda que las instituciones cuenten con elementos que aseguren la efectividad y eficiencia de las operaciones, la confiabilidad de la información y el cumplimiento de leyes y regulaciones.

Las disposiciones emitidas por la Superintendencia de Bancos y Seguros del Ecuador señalan que las instituciones controladas deberán implementar planes de continuidad, a fin de garantizar su capacidad para trabajar en forma permanente y minimizar las pérdidas en caso de interrupción de sus operaciones.

Las instituciones financieras requieren adoptar medidas preventivas para minimizar la probabilidad de ocurrencia de contingencias que afecten el normal desarrollo de sus operaciones, especialmente en la actualidad cuando la tecnología de la información es su activo más importante.

Frente a la posible ocurrencia de desastres, interrupciones o contingencias que pueden originar que los negocios financieros se suspendan o no se reestablezcan dentro de los plazos requeridos, es necesario contar con planes de continuidad y contingencia que permitan fortalecer las estructuras organizacionales.

Las entidades financieras públicas al tener un enfoque eminentemente social, deben mantenerse vigentes y cumplir con los objetivos por los cuales fueron creadas, por lo que es necesario se implementen políticas de gestión de riesgos, que les permitan sostenerse en el tiempo.

1.2.- FORMULACIÓN DEL PROBLEMA

El Banco Ecuatoriano de la Vivienda requiere disponer de medidas preventivas que garanticen que sus actividades están debidamente salvaguardadas y su continuidad garantizada, por lo que es preciso se cuenten con planes adecuados para cumplir con este objetivo.

Es necesario que para desarrollar el plan de continuidad del BEV se defina una metodología que incluyan las mejores prácticas para la gestión de riesgos, esta debe ser congruente con las metas, visión y cultura de riesgos de la entidad.

El desarrollo del tema propuesto tiene su justificación en la necesidad de que el BEV alcance la implementación de las mejores prácticas de riesgo operacional, a través del diseño de una metodología en donde se establezcan los lineamientos de políticas, procedimientos, prácticas y estructuras organizacionales que servirán para garantizar razonablemente que los objetivos del negocio sean alcanzados y que eventos no deseables sean prevenidos, detectados o corregidos.

1.3.- HIPÓTESIS

El BEV se encuentra implementando las mejores prácticas de riesgo operativo dado su carácter de banca pública y su especificidad orientada al segmento vivienda.

1.4.- PROCESAMIENTO DE LA INFORMACIÓN

Este estudio se lo efectuó en el Banco Ecuatoriano de la Vivienda, en donde se analizaron los riesgos que podría enfrentar y los procesos críticos con el fin de establecer herramientas apropiadas para la estructuración de los planes de continuidad y contingencia.

El BEV no cuenta con técnicas adecuadas que permitan establecer las etapas a seguir para la obtención de planes de contingencia y continuidad de los negocios.

Para el análisis propuesto se empleó la información existente en el banco correspondiente a: el plan estratégico 2010-2015, los procesos existentes, los informes de

auditoría interna, los informes presentados por el Comité Integral de Riesgos, los informes presentados por el Comité de Auditoría.

De acuerdo a la formulación del problema planteado esta investigación corresponde a un estudio descriptivo, que busca identificar las características de las mejores prácticas de riesgo operativo y de continuidad del negocio, para así establecer las particularidades que pueden ser aplicadas en el desarrollo de la metodología del plan de continuidad del BEV.

El método que se utilizó fue el de análisis, ya que se examinaron las posibles causas que pueden hacer que la entidad deje de operar y los efectos que llevarían a la suspensión forzosa de actividades del BEV.

Las fuentes primarias de información que se emplearon son: las encuestas, las entrevistas y la observación.

Las fuentes secundarias que se utilizaron para el desarrollo del tema propuesto son: las mejores prácticas de riesgos operacionales y planes de continuidad, las normas de la Superintendencia de Bancos y Seguros del Ecuador, textos que se relacionan con la gestión de riesgo operativo y documentos en donde se aborda el proyecto a ser planteado en el presente estudio.

1.5.- LIMITACIÓN Y ALCANCE DEL TRABAJO

Como se mencionó anteriormente, el presente trabajo trata de dar una guía para que la institución desarrolle sus planes de contingencia y continuidad de los negocios, dada la complejidad del tema es el BEV quien deberá efectuar los análisis pertinentes para la implementación de la metodología propuesta.

INTRODUCCIÓN

En los siguientes capítulos se realizará el análisis de las mejores prácticas de gestión de riesgos respecto a la implementación de planes de continuidad de los negocios, se describen los puntos principales de cada práctica y su importancia dentro del riesgo operativo.

En el capítulo III se presenta la estructura organizacional del BEV, se detallan los procesos por áreas de negocio y se describen los riesgos a los que está expuesta la institución, se analiza cualitativamente el impacto y la probabilidad de ocurrencia de los eventos de riesgo determinados.

En el cuarto capítulo se detallan las fases propuestas para la implementación de los planes de continuidad de los negocios, considerando las características del banco, las mejores prácticas y los requerimientos del organismo de control, se explican las bases técnicas necesarias para la obtención de la información, se entregan formularios que deberán ser llenados para la obtención de datos y la conformación del comité responsable de llevar a cabo los procesos de continuidad de los negocios.

En el quinto capítulo se describe el alcance que se espera tengan los planes de contingencia de la entidad, se establece la metodología a ser aplicada, se estructura la manera de determinar los riesgos asociados a los procesos críticos, se detallan pormenorizadamente las fases a ser ejecutadas para la obtención de los planes, se indica la estructura con que deben contar los planes de contingencia.

En el sexto capítulo, se presentan las conclusiones y recomendaciones que se entregarían a la institución con el fin de que la metodología propuesta pueda ser aplicada correctamente.

2. ANTECEDENTES

2.1 MEJORES PRÁCTICAS Y TEORÍAS APLICADAS

La planificación de la continuidad del negocio, (*Business Continuity Plan –BCP-*), es "el proceso mediante el cual las instituciones de servicios y financieras se aseguran de mantener o recuperar sus operaciones, incluyendo servicios al cliente, cuando confrontan eventos adversos tales como desastres naturales, fallas tecnológicas, errores humanos o terrorismo"[1]. Otro concepto del plan de continuidad del negocio dado por *The Business Continuity Institute,* señala que: "es un proceso continuo de administración y gobernabilidad, soportado por la alta gerencia y provisto de recursos para asegurar que son dados los pasos necesarios para identificar el impacto de pérdidas potenciales, mantener las estrategias y planes de recuperación viable y asegurar la continuidad de los productos y servicios mediante el ejercicio continuo, la aplicación práctica, pruebas recurrentes, capacitación mantenimiento y aseguramiento". El segundo concepto al reconocer que el proceso de continuidad del negocio es responsabilidad directa de la alta administración de una institución, refiere la importancia de contar con un gobierno corporativo que asuma la gestión de riesgos dentro de su accionar, lo cual es imperativo para la continuidad de sus operaciones.

Los objetivos de un plan de continuidad del negocio son: proteger las vidas humanas, tomar decisiones efectivas en tiempos de crisis, reducir la dependencia del personal específico, disminuir la pérdida de datos, utilidades y clientes, recuperar oportunamente las operaciones, mantener la imagen pública y la reputación de las empresas, mantener la capacidad para cumplir con las leyes y regulaciones aplicables.

Las fases requeridas para la implementación de los planes de continuidad son: la planificación del proyecto, el levantamiento de procesos o mapeo de procesos, el análisis de riesgos (*Risk Analysis* – RA-), el análisis de impacto en el negocio (*Business Impact Analysis* – BIA-), el diseño de estrategias, la capacitación y comunicación, la ejecución de pruebas, el

[1] José Israel Castro, *Administración de la Continuidad del Negocio*, Conferencia Alemana de Cooperativas, San José Costa Rica, 2007, p. 2.

mantenimiento y la actualización de los planes.

El BCP se centra en determinar la cadena de valor de la empresa y en encontrar cuales son los procesos críticos para el negocio, cuya interrupción puede afectar directamente los objetivos estratégicos de la organización, para lo cual determina las amenazas de acuerdo a las características del negocio y las selecciona de acuerdo a la mayor probabilidad de ocurrencia y a su impacto.

El desarrollo de los planes de contingencia y de continuidad de negocios, requieren en su aplicación de varios elementos que permitan definir su eficiencia y efectividad. De esta manera, se debe citar que su sustento deberá ser respaldado y promovido desde la principal autoridad de la organización hasta el personal de menor rango, manteniendo una cobertura que incluya colaboradores, proveedores y clientes.

Dentro de las premisas para la implantación de los planes de continuidad del negocio tenemos las siguientes:

- La alta gerencia de la organización debe establecer el presupuesto con el que va a contar para recuperar el negocio, es decir debe cuantificar las pérdidas si el negocio dejaría de funcionar y determinar el costo-beneficio que le generaría la implantación de un BCP.

- El BCP abarca todos los aspectos de la empresa, adicionalmente siempre debe estar actualizado y disponible.

- El BCP es un proceso continuo, debe ser ejecutado en forma continua.

- La estructuración de estrategias de recuperación se basa en el establecimiento de prioridades que dependen del giro del negocio.

- Se necesita un plan de concienciación, capacitación, pruebas y ejercicios, ya que todos los miembros de la organización deben conocer el rol que desempeñarán

dentro del plan de continuidad del negocio.

En la Resolución de la Superintendencia de Bancos No. JB-2005-834 se menciona que un plan de continuidad del negocio incluye un plan de contingencia, un plan de reanudación y un plan de recuperación.

Un plan de contingencia es el conjunto de procedimientos alternativos a la operativa normal de cada organización, cuya finalidad es la de permitir el funcionamiento de ésta, aún cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente interno o ajeno a la organización, este plan se lo efectúa de forma específica para un determinado factor de riesgo; el plan de contingencia se ejecuta el momento en el que se produce el evento y es efectuado por los técnicos y la parte operativa de las instituciones.

Los planes de reanudación especifican los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del evento; mientras que los planes de recuperación indican los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución.

A continuación se detallan las mejores prácticas para el desarrollo de los planes de contingencia y continuidad de los negocios:

2.1.1 Código de buenas prácticas de la gestión de continuidad del negocio BS 25999

El estándar BS 25999 es un código de buenas prácticas británico para la estructuración de los Sistemas de Gestión de la Continuidad del Negocio (*Business Capacity Management-BCM-*) en las empresas, intenta servir de referencia para la identificación de controles en la mayoría de situaciones donde el BCP es necesario, es usado en pequeñas, medianas y grandes organizaciones dedicadas a la industria, el comercio y el sector público.

Este estándar señala que existen tres temas clave para la administración de la continuidad: la resiliencia, el método probado y que efectivamente se gestione la continuidad del negocio.

De acuerdo al BS 25999 la resiliencia es: “La habilidad de una organización de resistir (y sobrevivir) cuando es afectada por un incidente”.

En base a lo indicado se establece que el Sistema de Gestión de Continuidad del Negocio, es un proceso del negocio, que establece un marco estratégico y operativo adecuado que: mejora la resiliencia de una organización contra la interrupción de la capacidad de alcanzar sus objetivos clave; proporciona un método probado de restauración, de la habilidad de una organización de proveer productos y servicios claves en un nivel convenido dentro de un plazo acordado después de una interrupción; entregando una capacidad probada de gestión de continuidad del negocio, cuyo fin es el de proteger a la organización y su reputación.

Para la implantación de un BCM se considera la mejora continua del Sistema de Gestión de la Continuidad del Negocio a través del *Ciclo Deming,* en el se presentan las siguientes fases:

- La planificación, en donde se establecen: políticas, objetivos, el alcance del plan, los recursos humanos con que se van a contar, los procesos y los controles adaptados a esos procesos y el presupuesto con que va a operar el BCM.
- La implementación y operación de esas políticas, procesos y controles.
- El monitoreo y la revisión de la ejecución de políticas y controles implementados de acuerdo a lo planificado.
- El mantenimiento y el mejoramiento del BCM, a través de la ejecución de acciones preventivas y correctivas.

2.1.2 Principios del Comité de Basilea

El Comité de Basilea promueve una mayor consistencia en la forma en que los bancos y las entidades reguladoras bancarias consideran la administración del riesgo fuera de las fronteras nacionales. Adicionalmente presenta recomendaciones para garantizar la adopción y aplicación de prácticas adecuadas de gobierno corporativo.

El Comité de Basilea, en diciembre de 2005, presenta su documento *"High-level principies for business continuity"*, en el se aborda la importancia de mantener un plan de continuidad en las instituciones financieras y señala que un manual de continuidad del negocio deberá incorporar: un análisis del impacto del negocio, las estrategias de recuperación basados en la revisión de los objetivos institucionales y el documento del plan de continuidad del negocio.

Adicionalmente establece siete principios que deberán ser aplicados en las organizaciones para contar con un adecuado plan de continuidad del negocio:

GRÁFICO No 1

Principios de Basilea a ser aplicados en la elaboración de los planes de continuidad del negocio

Elaboración: María Elena Ochoa **Fuente: Comité de Basilea**

2.1.2.1 Principio 1.- Responsabilidades del Directorio y de la Alta Administración.

El plan de continuidad del negocio debe ser una parte de la administración integral de riesgos de la industria financiera y de los negocios financieros, debe considerar tanto los planteamientos técnicos como la importancia del recurso humano en la organización.

El directorio es el responsable de gestionar la efectividad del plan de continuidad, para lo cual es necesario dicte políticas apropiadas con el fin de promover el reinicio y la continuidad de las operaciones, adicionalmente es el encargado de crear y promover una

cultura organizacional cuya mayor prioridad sea la continuidad del negocio, a través de la provisión necesaria de recursos tanto físicos como humanos.

La alta administración será el responsable de la comunicación organizacional, de asignar prioridades y recursos durante la interrupción de las actividades normales de la empresa.

2.1.2.2 Principio 2.- Interrupciones operacionales importantes.

La recuperación de las actividades de las instituciones financieras debe considerar sus principales características y perfiles de riesgo, porque así podrán disponer de los recursos necesarios de acuerdo a sus necesidades, las instituciones deben identificar el impacto de la interrupción de sus operaciones, con lo que se logrará una apropiada recuperación de los objetivos de su negocio.

Las autoridades financieras deben monitorear el mercado financiero y a los participantes en este sistema financiero, debido a su importancia global, es por esto que deberían coordinar los esfuerzos de las entidades por recobrar los servicios críticos del sistema financiero.

2.1.2.3 Principio 3.- Objetivos del reinicio de operaciones

Las autoridades financieras deben establecer los objetivos de recuperación que hagan que los riesgos del negocio disminuyan o desaparezcan para todo el sistema financiero.

La responsabilidad de la implementación de los objetivos de recuperación descansan en la alta administración de la organización, quienes deberán determinar los tiempos máximos de recuperación, dependiendo del impacto en la interrupción de sus operaciones, considerando los plazos máximos que el sistema financiero soportaría esta suspensión.

Las autoridades financieras deberían considerar los diferentes riesgos en los que las organizaciones podrían incurrir durante la interrupción de sus servicios críticos, tales

como: la pérdida de los archivos de sus transacciones, los inconvenientes de liquidez, los problemas de solvencia y la pérdida de confidencialidad.

Los objetivos de recuperación deben identificar los niveles de expectativas y los tiempos de recuperación para actividades específicas, para lo cual se contará con herramientas como el *benchmarks*, lo cual ayudará a probar la efectividad de los planes de continuidad en otras organizaciones.

Cuando se identifican los objetivos de recuperación entonces se pueden establecer los tiempos apropiados para la implementación de estos objetivos.

2.1.2.4 Principio 4.- Comunicación

Los participantes de la industria financiera y las autoridades financieras deben incluir en sus planes de continuidad del negocio la comunicación entre su organización y las partes externas en caso de la ocurrencia de eventos que provoquen interrupciones operacionales relevantes.

La comunicación efectiva entre las partes internas y externas de la organización, cuando suceden los eventos de mayor interrupción operacional, es esencial para los participantes de la industria financiera, principalmente en la etapa inicial, ya que si se logra efectuarla se disminuirá el impacto para así tomar las mejores decisiones acerca de la aplicación de los planes de continuidad. La confidencialidad de la información que deben mantener los participantes del sistema financiero requiere que la comunicación sea clara y regular cuando los eventos de mayor impacto estén sucediendo.

Los planes de continuidad de las entidades financieras y las autoridades financieras deben incorporar protocolos y procedimientos de comunicación de emergencia. Las autoridades financieras deben considerar que estos procedimientos de comunicación son de su responsabilidad.

Los procedimientos de comunicación de los participantes del sistema financiero y sus

autoridades, generalmente deben:

Identificar a los responsables de la comunicación entre el staff y los accionistas. Este grupo deberá estar conformado principalmente por: el gerente, relaciones públicas, consejeros legales de cumplimiento y un responsable del staff encargado de la organización de los procesos de continuidad del negocio. Este debe siempre mantenerse en comunicación, localizado en diferentes lugares o en los sitios en donde se encuentren las funciones primarias del negocio.

La existencia de protocolos de comunicación en los sistemas financieros incluyen la información de los contactos de las autoridades financieras y de los participantes de la industria financiera, que faciliten las condiciones para que el sistema coordine sus esfuerzos de recuperación.

Señalar las direcciones de los recursos que pueden perderse durante las mayores interrupciones operacionales, así como la manera en que se responderá a los inconvenientes presentados en los sistemas de comunicación importantes. Proveer una actualización regular de los contactos de información.

2.1.2.5 Principio 5.- Comunicación entre instituciones de otras jurisdicciones.

Los procedimientos de comunicación de los participantes de la industria financiera y sus autoridades y los participantes de las instituciones financieras de otras jurisdicciones en los eventos de mayores interrupciones operacionales tienen implicación fuera del país de origen.

Este hecho se origina en la interdependencia de los participantes de la industria financiera, el impacto de las mayores interrupciones se extienden más allá de las fronteras de un país.

Las autoridades deberían incluir en sus protocolos de comunicación de sus planes de negocio la manera en que se comunicarán con las autoridades de otras jurisdicciones en

el caso de que sucedan mayores interrupciones operacionales.

2.1.2.6 Principio 6.- Pruebas

Las autoridades de las industrias que participan en el sistema financiero y las supervisoras deben evaluar sus planes de continuidad del negocio, si los manuales de continuidad del negocio son efectivos.

Se deben efectuar pruebas periódicas para comprobar la habilidad de las organizaciones para recobrar sus operaciones críticas, que son un componente esencial de los manuales de continuidad del negocio. Se determinará el alcance y la frecuencia de las aplicaciones críticas en las operaciones de las instituciones, además se establecerá la necesidad de modificar los planes de continuidad del negocio, si es necesario efectuar una auditoría externa o interna, resultados que serán reportados al directorio institucional.

La decisión de la aplicación de determinadas acciones en el plan de continuidad del negocio debería determinarse a través de un análisis de costo – beneficio para la organización.

2.1.2.7 Principio 7.- Los Manuales de Continuidad del Negocio deben ser revisados por los supervisores.

Los supervisores deberían esperar que los participantes en la industria financiera desarrollen e implementen planes de continuidad del negocio viables y apropiados a la realidad de cada organización. Estos deberán considerar el alcance y la frecuencia de su supervisión con el fin de determinar los requerimientos de sus regulaciones.

2.1.3 Ley de Sarbanes-Oxley (SOX)

La Ley Sarbanes Oxley (*Sarbanes Oxley Act*) fue aprobada por el Congreso de los Estados Unidos en el mes de Octubre del 2002. “El principal objetivo de esta ley es regular las funciones financieras, contables y de auditoría, penalizando de una forma severa, el fraude

corporativo, la corrupción administrativa, los conflictos de interés, la negligencia y la mala práctica de los altos directivos"[2]. Para lograr este objetivo la Ley creó un nuevo organismo supervisor de la contabilidad (*Public Company Accounting Oversight Board - PCAOB*) el mismo que estableció nuevas reglas de independencia del auditor reformando la contabilidad corporativa.

La Ley Sarbanes Oxley es un texto cuyos contenidos principales se agrupan en seis grandes áreas que afectan a todas las sociedades. A continuación, se mencionan algunos de los requisitos más importantes, en relación con cada una de éstas áreas:

2.1.3.1 Mejora de la calidad de la información pública.-

La Ley establece que los Gobiernos Corporativos de las compañías deberán certificar su responsabilidad por la información acerca de la efectividad de los procesos de control interno que se presenta trimestral y anualmente a la SEC (Sección 302). Adicionalmente, se establece la presentación de un informe en donde se indique si han existido cambios significativos en el control interno y en la información que se comunica a los mercados (Sección 409).

En estas secciones de la Ley también se establecen nuevos requerimientos de control que incluyen la obligatoriedad de la evaluación del control interno por parte del auditor externo, el cual opinará sobre la corrección de lo manifestado por la sociedad sobre la eficiencia del control interno financiero a la fecha de cierre de los estados financieros (Sección 404).

2.1.3.2 Reforzamiento de las responsabilidades del Gobierno corporativo de las empresas.-

La Ley promueve la creación de los Comités de Auditoría compuestos por asesores independientes quienes serán los responsables de supervisar el trabajo del auditor (Sección 301) y deberán mantener comunicaciones directas en temas de vital

[2] U.S Securities and Exchange Comission, *SEC Initiatives Under New Regulatory Reform Law*, pag. 4

importancia como las políticas y tratamientos contables de la empresa (Sección 204). Adicionalmente, se establece la obligación de contar con expertos financieros en el Comité de Auditoría e informar a la SEC sobre quiénes son los consejeros que cuentas con esta experiencia (Sección 407).

2.1.3.3 Mejora en las conductas y comportamientos éticos exigibles.-

En estas secciones la Ley impone mayores exigencias de responsabilidad en temas de gestión indebida de información confidencial (Sección 403). También, se establece la obligatoriedad de tener un Código de Ética para los Ejecutivos del Área Financiera, en donde los cambios o incumplimientos a este código deben ser informados públicamente (Sección 406). Además, se implanta la protección especial para los denunciantes anónimos de conductas ilícitas e irregulares de la sociedad.

2.1.3.4 Aumento de la supervisión a las actuaciones en los mercados cotizados.-

Creación de un organismo público de supervisión denominado: *Public Company Accounting Oversight Board* (PCAOB) (Sección 101 y 102) "Comisión que tiene la capacidad de registrar, supervisar y establecer estándares de auditoría, controles de calidad, normas de ética e independencia de los auditores externos"[3]. Adicionalmente, en estas secciones se establece una extensión de las responsabilidades profesionales de los abogados quienes están obligados a informar inmediatamente a la SEC de cualquier violación material de las leyes financieras por parte de las empresas (Sección 407).

2.1.3.5 Incremento del régimen sancionador relacionado con el incumplimiento.-

En estas secciones de la Ley, se extiende el plazo en que se puede perseguir un fraude cometido y/o identificado (2 años después del descubrimiento de los actos que constituyen la violación o 5 años después de dicha violación). (Sección 804). Además, se establece la obligación para la alta dirección (CEO y CFO) de certificar, bajo

[3] José Díaz Morales, *La Ley Sarbanes Oxley y la Auditoría*, Ernst & Young LLP, 2004, pp. 4.

responsabilidad penal, su buena fe en cuanto a que los informes públicos: cumplen con todos los requisitos establecidos en la Ley, presentan en todos aspectos materiales, la situación financiera y los resultados de las operaciones de la empresa. (Sección 906). Por último se establece un aumento importante de las sanciones por no testificar, facilitar información o cooperar con las investigaciones oficiales, y por la alteración de documentos o registros con el fin de obstruir o impedir una investigación (Sección 802 y 1102).

2.1.3.6 Aumento de la exigencia y presión sobre la independencia de los auditores externos

En la Ley existen varias secciones dedicadas a normar la relación entre las empresas y el auditor externo. Estas secciones buscan, principalmente, mantener la independencia del auditor, con el objetivo de evitar que se repitan eventos como el escándalo de Enron (2001) en el que se confirmó la complicidad de la firma auditora Arthur Andersen. Entre algunos de los requerimientos que fueron introducidos en la Ley se menciona: La prohibición total para que el auditor externo pueda prestar determinados servicios complementarios a sus clientes de auditoría (Sección 201); la rotación cada 5 años de los ejecutivos del equipo de auditoría (socio firmante y el socio revisor) (Sección 203); el establecimiento de restricciones importantes para que una entidad contrate personal del equipo de auditoría externa (se establece un periodo "de enfriamiento" (cool off) de un año en el que no se pueden producir estas contrataciones para puestos clave en relación directa (Sección 206).

2.1.4 Cobit

"El gobierno de Tecnología de la Información (TI) es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que la TI de la empresa sostiene y extiende las estrategias y objetivos

organizacionales." [4]

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT) entregan buenas prácticas a través de un marco de trabajo de dominios y procesos. Está enfocado en el control y menos en la ejecución. Estas prácticas ayudan a optimizar las inversiones en la Tecnología de la Información, TI, aseguran la entrega del servicio y brindan una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que la TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implantar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

• Estableciendo un vínculo con los requerimientos del negocio

• Organizando las actividades de TI en un modelo de procesos generalmente aceptado

• Identificando los principales recursos de TI a ser utilizados

• Definiendo los objetivos de control gerenciales a ser considerados.

La orientación al negocio que enfoca COBIT consiste en vincular las metas de negocio con las metas de TI. COBIT da soporte al gobierno de TI al brindar un marco de trabajo que garantiza que:

• La Tecnología de la Información está alineada con el negocio.

• La Tecnología de la Información capacita el negocio y maximiza los beneficios.

• Los recursos de TI se usan de manera responsable.

• Los riesgos de TI se administran apropiadamente.

Los productos COBIT se han organizado en tres niveles diseñados para dar soporte a:

---

[4] Cobit 4.0, *Objetivos de Control Directrices Generales Modelos de Madurez*, IT Governance Institute, pag. 6

• La administración y consejos ejecutivos.

• La administración del negocio y de TI.

• Los Profesionales en Gobierno, aseguramiento, control y seguridad.

Las mejores prácticas de TI se han vuelto significativas debido a:

• Los directores del negocio y los consejos directivos demandan un mayor retorno de la inversión en TI.

• La necesidad de satisfacer requerimientos regulatorios para controles de TI en áreas como privacidad y reportes financieros (por ejemplo, Ley de Sarbanes Oxley, Basilea II) y en sectores específicos como el financiero, farmacéutico y de atención a la salud.

• La selección de proveedores de servicio y el manejo de *outsourcing* y de adquisición de servicios.

• Los riesgos complejos de la TI como los que se pueden encontrar en la seguridad de redes.

• Iniciativas de gobierno de TI que incluyen la adopción de marcos de referencia de control y de mejores prácticas para ayudar a monitorear y mejorar las actividades críticas de TI, aumentar el valor del negocio y reducir los riesgos de éste.

• La necesidad de optimizar costos siguiendo, un enfoque estandarizado en lugar de enfoques desarrollados especialmente.

• La necesidad de las empresas de valorar su desempeño en comparación con estándares generalmente aceptados y con respecto a su competencia.

2.1.5 Coso

El documento "Gestión de Riesgos Corporativos, Marco Integrado" -elaborado por el *Comitee of Sponsoring Organizations of the Treadway Comisión-* proporciona a la

administración de las entidades: criterios prácticos y ampliamente aceptados para la elaboración de sistemas y procedimientos de control interno, un marco para la evaluación de su eficiencia a través del tiempo, principios que promueven la transparencia de la información financiera y la responsabilidad de la administración.

El COSO es la metodología más actualizada y completa que existe para la evaluación del control interno de las organizaciones, su principal ventaja se relaciona con la incorporación del análisis del riesgo, la amplia difusión y conocimiento de los Gobiernos Corporativos, la aplicabilidad a todo tipo de empresas y la aceptación de sus resultados por parte de las entidades de control.

El COSO establece como componentes del control interno a: el monitoreo, la información y comunicación, las actividades de control, la evaluación de riesgos y el ambiente de control, estos componentes a su vez están interrelacionados e integrados al proceso de administración de las instituciones.

2.1.6 Estándar ISO/IEC 27002

Es un estándar publicado por la Organización Internacional para la Estandarización, y por la Comisión Internacional Electrotécnica, relacionada con la seguridad de la información, constituye un código de prácticas aplicadas para la tecnología de la información.

Habla sobre la preservación de la información que debe ser: confidencial, integra y disponible de acuerdo a las autorizaciones de los usuarios de la organización.

En este estándar existe un acápite relacionado con los aspectos de la seguridad de la información en la gestión de continuidad del negocio, en el se indican los objetivos de contrarrestar las interrupciones en las actividades del negocio y proteger los procesos críticos contra los efectos de fallas importantes en los sistemas informáticos y asegurar la recuperación oportuna de la información.

Señala que “la gestión de continuidad del negocio debería incluir controles para

identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, limitar las consecuencias de los incidentes dañinos y garantizar la disponibilidad de la información requerida para los procesos del negocio"[5]

A continuación se detallan los procesos de la seguridad de la información en la gestión de continuidad:

2.1.6.1. Inclusión de la seguridad en el proceso de gestión de la continuidad del negocio

El control en la seguridad de la información a establecerse deberá desarrollar y mantener un proceso de gestión de la continuidad del negocio en toda la organización

2.1.6.2. Continuidad del negocio y evaluación de riesgos

Las instituciones deberán identificar los eventos que puedan ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de ocurrencia de las interrupciones, y las posibles consecuencias para la seguridad de la información.

2.1.6.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

Con el objetivo de mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el tiempo requerido, después de la interrupción de los procesos críticos para el negocio.

2.1.6.4. Estructura para la planificación de la continuidad del negocio:

Para asegurar que los planes son consistentes se deberá mantener una sola estructura de continuidad, en donde se establecerán los requisitos de seguridad de la información y la identificación de prioridades para la implementación de pruebas y mantenimiento del plan.

---

[5] Norma Técnica Ecuatoriana, NTE INEN-ISO/IEC 27002:207009, *Tecnología de la Información-Técnicas de la Seguridad, Código de Practica para la Gestión de la Seguridad de la Información*, pag. 94.

2.1.6.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio:

Los planes de continuidad deberán someterse a pruebas periódicas para asegurar su eficiencia, adicionalmente deberán establecerse procesos de mantenimiento y actualización.

3. ANÁLISIS DE LA SITUACIÓN ACTUAL DEL BEV

3.1. ANTECEDENTES

Desde su fundación en el año 1961 el BEV se ha enfocado en el desarrollo de productos financieros destinados a facilitar el acceso a una vivienda digna para la población en Ecuador. Esta perspectiva se encuentra orientada en mejorar la calidad de vida de los habitantes del país, permitiéndoles alcanzar fuentes de financiamiento viables en función de sus posibilidades económicas para la adquisición de vivienda.

El Banco Ecuatoriano de la Vivienda a partir del año 1992 cambia sus operaciones a banca de segundo piso, esta decisión se sustenta en que se determinó que la institución debería cambiar el rol de provisionador y financiador directo de soluciones habitacionales, hacia el de facilitador, energizador y sustentador de las actividades del sector privado tanto formal como informal dentro del desarrollo habitacional.

Bajo este contexto la entidad definió nuevos esquemas que permitieron financiar proyectos de vivienda de interés social, por lo que se crean varios productos, tales como: el redescuento de cartera inmobiliaria de instituciones financieras, los fideicomisos inmobiliarios, el crédito a constructores y el crédito a gobiernos seccionales.

En el año 2010 el Banco Central del Ecuador, con fondos de la Reserva de Libre Disponibilidad, realizó una inversión doméstica de USD 100 MM al BEV. Con base en el flujo originado en tales depósitos a plazo, el BEV aprobó créditos para el desarrollo de proyectos inmobiliarios de interés social a través del producto crédito a constructores y cuenta al 31 de mayo de 2011 con una cartera de proyectos de USD 62MM aproximadamente.

Su fortaleza patrimonial le ha llevado a tener una calificación BBB+[6] dada en función de escala nacional que evalúa el riesgo institucional basado en sus activos, pasivos y patrimonio.

[6] Calificación otorgada por la firma Bank Watch Ratings, marzo 2011.

3.2. IDENTIFICACIÓN DE LOS EVENTOS DE RIESGO

El constante cambio en la administración del BEV ha sido uno de los principales problemas que han ocasionado que la institución no cuente con políticas de gestión a mediano y largo plazo.

El mapeo estructural de la institución se encuentra en proceso de desarrollo y diagramación. No ha existido durante este desarrollo una aplicación sistematizada mediante una metodología única definida, situación que no ha permitido manejar una estandarización en los diagramas realizados dificultando la identificación de las rutas criticas de cada proceso y por ende los eventos de riesgo a los que están sujetos.

Debido a este escenario, la necesidad de identificación de riesgos operativos es urgente y considerada elemental para sustentar un crecimiento sostenible de la institución, con el fin de velar por los intereses de sus clientes, empleados y proveedores.

Por esta situación uno de sus principales objetivos está basado en la implantación de un sistema de administración integral de riesgos que se enfoque principalmente en el desarrollo de los siguientes cambios:

- Desarrollar e implantar una cultura y comportamiento organizacional referente a una adecuada administración de riesgos.
- Establecer una plataforma única de información y comunicación que agilite la aplicación de los programas de prevención, emergencia y recuperación de riesgos.
- Consolidar políticas y procedimientos claramente definidos y en total conocimiento del personal a cargo de las diferentes áreas para garantizar una adecuada administración del riesgo minimizando sus causas y efectos.
- Establecer un sistema de control y monitoreo permanente que detecte las desviaciones presentadas en los procesos a fin de atender inmediatamente sus

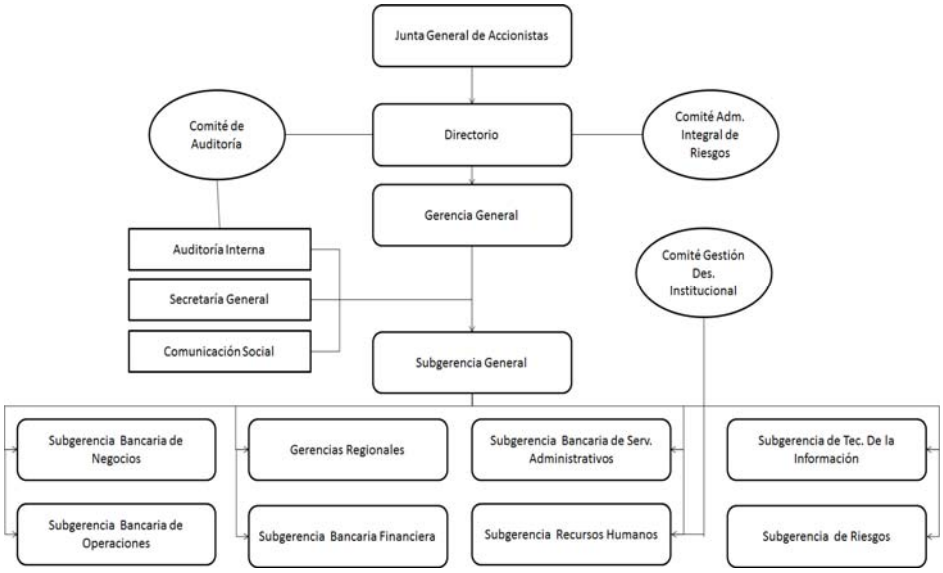
causas para minimizar los efectos producidos por la presencia de un factor interno o externo no controlable.

Basado en los objetivos propuestos, la identificación de los procesos y sus relaciones es fundamental, para posteriormente identificar los riesgos a presentarse con el fin de determinar los niveles de criticidad de los procesos.

3.2.1 Estructura orgánica funcional del BEV

GRAFICO No. 2

Estructura orgánica funcional del BEV



Fuente: BEV.

En el gráfico No. 2, se presenta el Organigrama Funcional del BEV, en donde se establecen las líneas jerárquicas de la organización, siendo su principal autoridad la Junta de Accionistas, luego encontramos al Directorio Institucional y la Gerencia General, a la cual asesoran directamente el Comité de Auditoría y el Comité de Administración Integral de Riesgos, la Subgerencia Jurídica se encuentra en directa relación con la Gerencia del BEV. De la Subgerencia General dependen el resto de áreas tanto operativas como administrativas.

3.2.2 Definición de la estructura por procesos de gestión

Conforme a la información existente, la visión de procesos se presenta mediante una clasificación técnica que evalúa la importancia y prioridad de las diferentes actividades contenidas en relación a sus usuarios. De esta manera, la estructura general de procesos es la siguiente:

Procesos gobernantes o estratégicos

Procesos creadores de valor

Procesos habilitantes

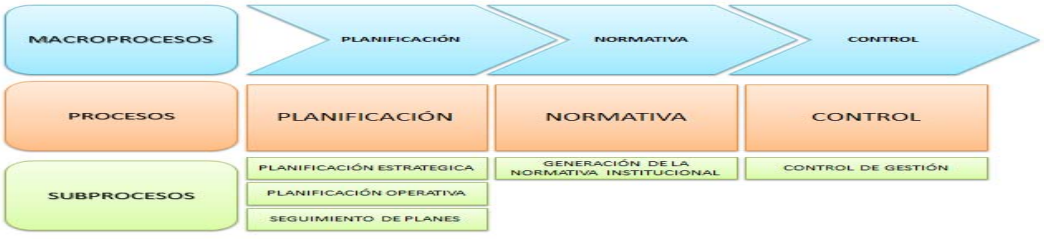
3.2.2.1 Procesos gobernantes o estratégicos:

"Se entiende como procesos gobernantes o estratégicos aquellos cuya incidencia y gestión afectan a toda la estructura de la organización, principalmente porque incluyen las áreas básicas de la administración dadas por la planificación, organización, dirección y control."[7]

Dentro de esta categoría se han definido tres macro procesos que contienen tres procesos y cinco subprocesos como se muestra en la ilustración desarrollada: [8]

GRAFICO No. 3

Procesos gobernantes o estratégicos



Elaboración: María Elena Ochoa **Fuente: BEV**

[7] Ana Fernandez Laviada, *La Gestión del Riesgo Operacional*, UCEIF Ediciones, 2010, p. 40.
[8] Levantamiento de Procesos BEV, Desarrollo Organizacional 2009.

3.2.2.2 Procesos creadores de valor

Se define como procesos creadores de valor a los concernientes a la razón propia de la existencia del BEV, conformada por dos macro procesos, cuatro procesos y dieciocho subprocesos como se muestra en la siguiente ilustración:

GRAFICO No. 4

Procesos creadores de valor

Elaboración: María Elena Ochoa **Fuente: BEV**

Como podemos observar en el gráfico No 4, los procesos de cartera y de fondeo son los pertenecientes a la cadena de valor de la institución.

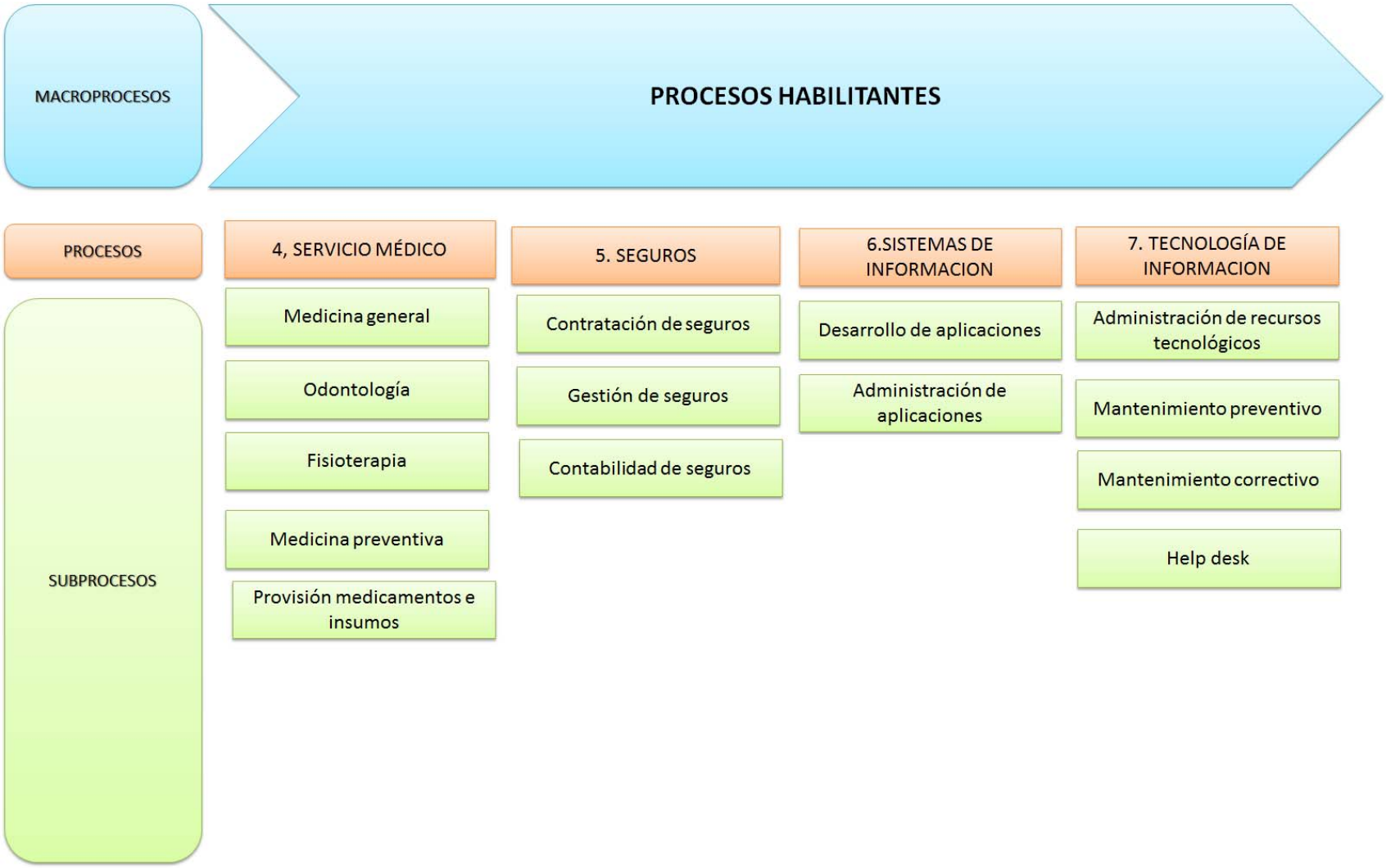
3.2.2.3 Procesos habilitantes

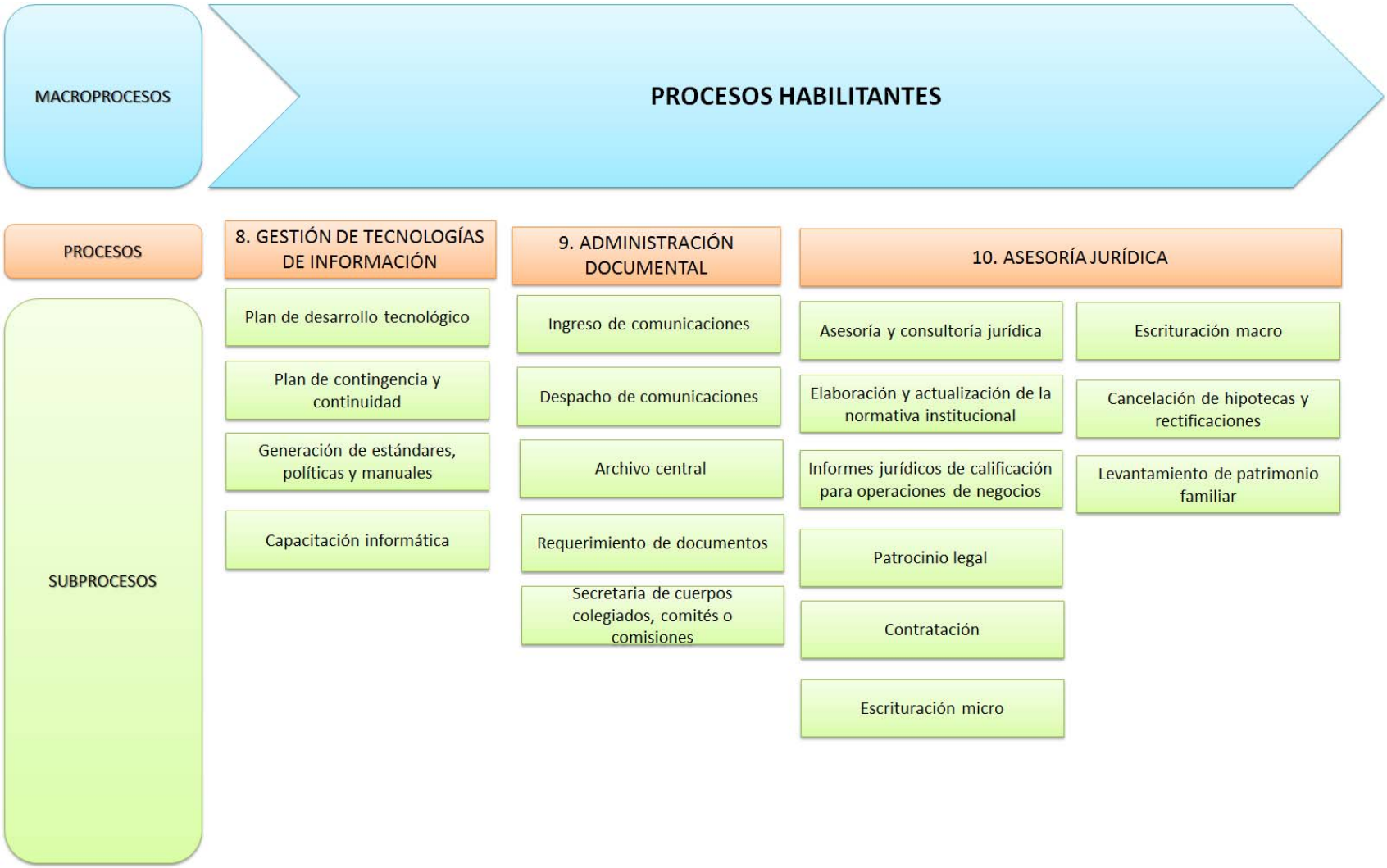
Los procesos habilitantes están conformados por aquellas áreas de apoyo que garantizan el funcionamiento de toda la organización. Su composición comprende un macroproceso, quince procesos y noventa y dos subprocesos.

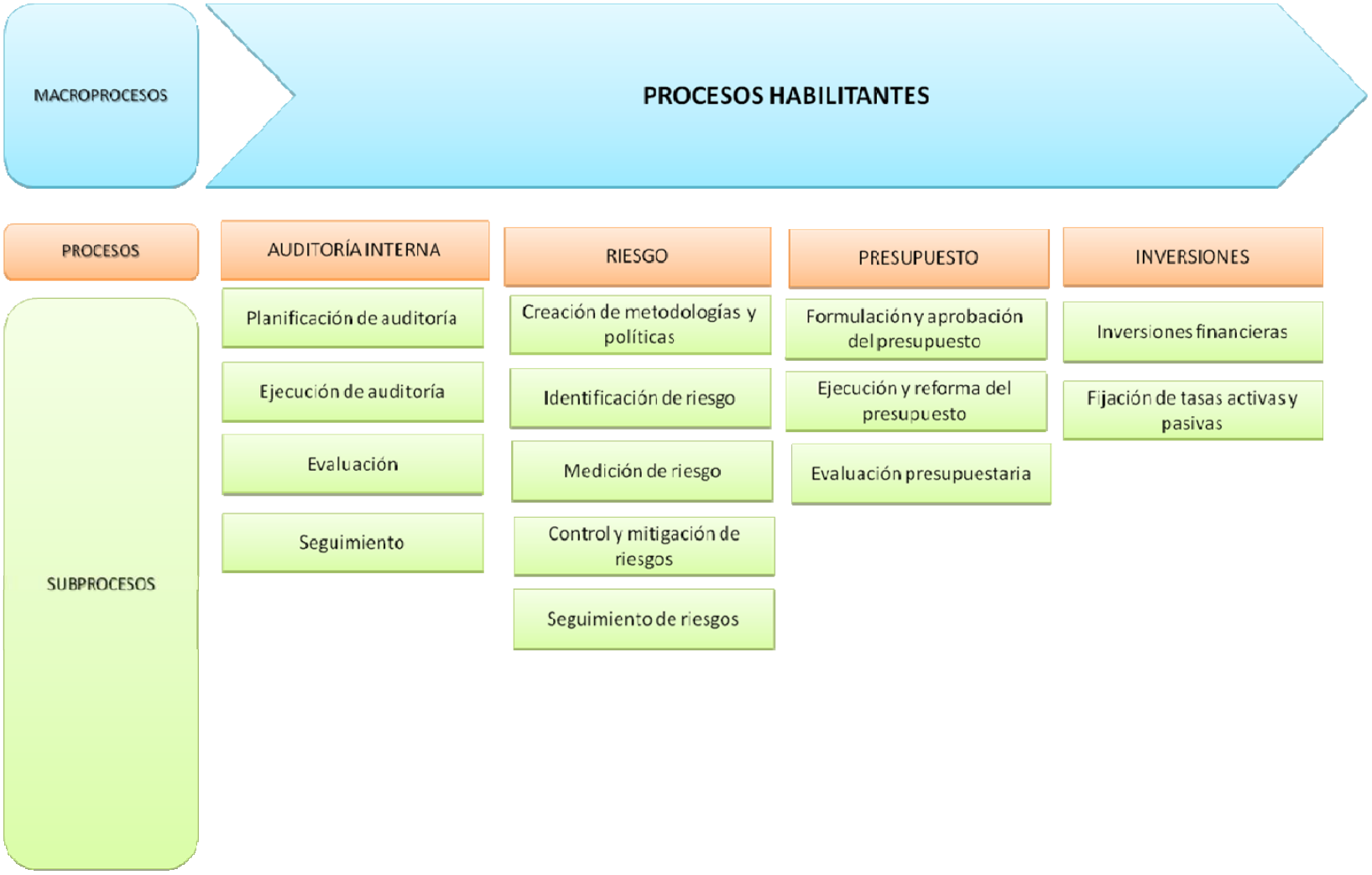
Como se observa los procesos habilitantes conforman la base operativa de la empresa, concentrando la mayor cantidad de recursos existentes, por lo que presentan riesgos de diferente variabilidad e importancia para el BEV.

GRAFICO No. 5

Procesos habilitantes


MACROPROCESOS
PROCESOS HABILITANTES
PROCESOS
SUBPROCESOS
4, SERVICIO MÉDICO
Medicina general
Odontología
Fisioterapia
Medicina preventiva
Provisión medicamentos e insumos
5. SEGUROS
Contratación de seguros
Gestión de seguros
Contabilidad de seguros
6.SISTEMAS DE INFORMACION
Desarrollo de aplicaciones
Administración de aplicaciones
7. TECNOLOGÍA DE INFORMACION
Administración de recursos tecnológicos
Mantenimiento preventivo
Mantenimiento correctivo
Help desk


MACROPROCESOS
PROCESOS HABILITANTES
PROCESOS
SUBPROCESOS
8. GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN
Plan de desarrollo tecnológico
Plan de contingencia y continuidad
Generación de estándares, políticas y manuales
Capacitación informática
9. ADMINISTRACIÓN DOCUMENTAL
Ingreso de comunicaciones
Despacho de comunicaciones
Archivo central
Requerimiento de documentos
Secretaria de cuerpos colegiados, comités o comisiones
10. ASESORÍA JURÍDICA
Asesoría y consultoría jurídica
Elaboración y actualización de la normativa institucional
Informes jurídicos de calificación para operaciones de negocios
Patrocinio legal
Contratación
Escrituración micro
Escrituración macro
Cancelación de hipotecas y rectificaciones
Levantamiento de patrimonio familiar


MACROPROCESOS
PROCESOS HABILITANTES
PROCESOS
SUBPROCESOS
AUDITORÍA INTERNA
Planificación de auditoría
Ejecución de auditoría
Evaluación
Seguimiento
RIESGO
Creación de metodologías y políticas
Identificación de riesgo
Medición de riesgo
Control y mitigación de riesgos
Seguimiento de riesgos
PRESUPUESTO
Formulación y aprobación del presupuesto
Ejecución y reforma del presupuesto
Evaluación presupuestaria
INVERSIONES
Inversiones financieras
Fijación de tasas activas y pasivas

Elaboración: María Elena Ochoa **Fuente: BEV**

3.2.3 Definición e identificación de los procesos críticos del BEV

La criticidad de los procesos en el BEV, se mide en función de la importancia de sus actividades en el cumplimiento de los objetivos propuestos y los riesgos existentes que pueden afectar su desenvolvimiento.

Toda la estructura presentada dispone de áreas críticas que pueden afectar el comportamiento general de la institución. De igual manera, todos los procesos pueden verse afectados por riesgos internos y externos diferentes a los riesgos de mercado, liquidez y de crédito, considerados tradicionales en este tipo de instituciones y que por lo general guardan una mayor atención y cuidado en su prevención y corrección. No obstante, muchos de estos factores operacionales pueden desarrollar impactos que alteren drásticamente la seguridad institucional poniendo inclusive en riesgo el cierre de operaciones del banco.

"Las falencias en los sistemas de información y los procesos internos pueden producir errores tanto en la gestión automatizada como en el recurso humano, situación que produce paralizaciones y pérdidas financieras que pueden expandirse a afecciones a los proveedores y clientes comprometiendo el desarrollo empresarial."[9]

Es por esto que la medición de criticidad toma en consideración la cultura y comportamiento organizacional y la gestión cualitativa y cuantitativa de la empresa dada principalmente por la incorporación de todos los recursos que hacen posible la gestión operativa del BEV.

"Mediante esta cobertura, se exponen a continuación los resultados existentes en cada área en base al siguiente modelo de medición:"[10]

BAJO	
MODERADO	
ALTO	
EXTREMO	

[9] Jairo Amaya Amaya, *Sistemas de Información,* ECOE Ediciones, 2005, p. 23
[10] Mauricio Baquero Herrera, *La Nueva Propuesta del Comité de Basilea, relacionada con Estándares de Supervisión Bancaria*, 2008, España, p.54

Las áreas descritas se fundamentan en el impacto de los riesgos a producir en relación a la probabilidad de ocurrencia de los mismos, en base a la siguiente descripción:

TABLA No 1

Medidas de consecuencia / impacto

Nivel	Descriptor	Ejemplo de Descripción Detallada
1	Insignificante	Sin perjuicios, baja pérdida financiera
2	Menor	Procesos levemente afectados o paralizados, Pérdida financiera media
3	Moderado	Procesos, afectados y paralizados, Pérdida financiera alta
4	Mayor	Procesos afectados considerablemente por agentes internos o externos Pérdida financiera mayor
5	Catastrófico	Procesos dañados, maquinaria destruida, riesgos graves de personal, enorme pérdida financiera

Elaboración: María Elena Ochoa **Fuente: Gestión de Riesgo Australiana**

TABLA No 2

Medidas cualitativas de probabilidad

Nivel	Descriptor	Descripción
A	Casi Certeza	Se espera que ocurra en la mayoría de las circunstancias
B	Probable	Probablemente ocurrirá en la mayoría de circunstancias
C	Posible	Puede ocurrir en algún momento
D	Improbable	Pudo ocurrir en algún momento
E	Raro	Puede ocurrir solo en circunstancias excepcionales

Elaboración: María Elena Ochoa **Fuente: Gestión de Riesgo Australiana**

En función del impacto y probabilidad se obtienen las calificaciones basadas en estos conceptos:

Bajo: Riesgo bajo. Se administra en función de procedimientos de rutina.

Moderado: Riesgo moderado, debe especificarse responsabilidad gerencial

Alto: Riesgo alto, necesita atención de alta gerencia

Extremo: Riesgo extremo, requiere acción inmediata de los responsables en función de la magnitud del daño. Los responsables pueden ser:

- El personal a cargo
- Los directivos del área
- Facilitadores externos contratados para recuperar los daños.

TABLA No 3

Análisis de nivel de riesgo

PROBABILIDAD	CONSECUENCIAS				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
A	ALTO	ALTO	EXTREMO	EXTREMO	EXTREMO
B	MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
C	BAJO	MODERADO	ALTO	EXTREMO	EXTREMO
D	BAJO	BAJO	MODERADO	ALTO	EXTREMO
E	BAJO	BAJO	MODERADO	ALTO	ALTO

Elaboración: María Elena Ochoa **Fuente: BEV**

3.2.3.1 Descripción del proceso de medición del riesgo operativo del BEV

Conforme a los rangos presentados, cada uno de los procesos corresponde a la medición cualitativa que establece la criticidad de los procesos.

3.2.3.1.1 Categorización de variables:

Las variables utilizadas para la medición del riesgo operativo, se clasifican en tres grupos:

a) Riesgo de personal:

El riesgo de personal se mide en función de la siguiente tabla de ponderación:

TABLA No 4

Riesgo de personal

(Ver siguiente página)

Sub Variables	Fórmula	Posibles respuestas
Recursos Suficientes	Recursos existentes/Recursos Demandados	>1 Eficiente (Revisión de sobre calificación) <1 Deficiente. No adecuado al cargo >1 Sobrecarga >1 Déficit de carga
Recursos Suficientes	Análisis de Cargas de Trabajo: Tiempo Efectivo + Tiempo de espera/ 8 Horas	>1 Eficiente (Revisión de sobre calificación) <1 Deficiente. No adecuado al cargo >1 Sobrecarga >1 Déficit de carga
Nivel de Capacitación	Nivel Existente/Nivel Requerido Competencias Disponibles/Competencias Requeridas Experiencia Disponible/Experiencia Requerida	>1 Eficiente (Revisión de sobre calificación) <1 Deficiente. No adecuado
Asignación de Responsabilidades	Índice de evaluación de rendimiento: Logros alcanzados/logros propuestos	>1 Rendimiento Aceptable >1 Rendimiento deficiente

Elaboración: María Elena Ochoa **Fuente: BEV**

b) Riesgo de Tecnología.

La tecnología se evalúa en función de las siguientes variables:

TABLA No 5

Riesgo de tecnología

Sub Variables	Fórmula	Ponderación
Integración	Una plataforma requerida/Nº Plataformas existentes	>1 Existencia de riesgo por falta de integración de datos
Estandarización	Lenguaje único de programación/ Lenguajes utilizados	>1 Existencia de riesgo por falta de integración de datos
Disponibilidad	Nivel de utilización/Nivel requerido de utilización	>1 Capacidad Tecnológica no utilizada

Elaboración: María Elena Ochoa **Fuente: BEV**

c) Riesgo de Procesos

Las variables utilizadas en la valoración del riesgo operativo son:

TABLA No 6

Riesgo de procesos

(Ver siguiente página)

Sub Variables	Fórmula	Ponderación
Políticas y Procedimientos	Existencia de Reglamentación/Áreas disponibles Nivel de cumplimiento	1 Cobertura Completa <1 Cobertura Deficiente Valoración de Rendimiento
Estandarización	Aplicación de Procedimientos de Prevención Aplicación de Procedimientos de Contingencia(Emergencia) Aplicación de Procedimientos de Recuperación	Índice de Cumplimiento mediante revisión con check list
Medición de tiempos de respuesta	Tiempo de Proceso=Tiempo Efectivo +Tiempo Muerto	Rangos de Deviación estándar para análisis de tiempos

Elaboración: María Elena Ochoa **Fuente: BEV**

3.2.3.1.2 Procesos críticos del área Financiera

El área Financiera por naturaleza se encuentra dentro de un entorno variable y de alta volatilidad debido a que está sujeta a cambios en el mercado, mismos que son totalmente impredecibles. Su control es exhaustivo aunque su enfoque principalmente se orienta a riesgos de mercado por lo que se vuelven muy vulnerables a riesgos internos que perjudican su ejecución.

A diferencia de otros procesos, estos responden no solo a políticas internas sino principalmente al cumplimiento de la legislación ecuatoriana referente a tributos, información e impuestos por lo que exigen exactitud en su cumplimiento. Cualquier error cometido puede alterar las cifras y mostrar resultados diferentes a la realidad que producen escenarios irreales e inexistentes.

Los riesgos actuales se detallan en la siguiente tabla:

TABLA No 7

Procesos críticos del área Financiera

(Ver siguiente página)

		VARIABLES DE RIESGO OPERACIONAL INTERNO						
CODIFICACION	SUBPROCESO	SISTEMA DE NFORMACIÓN	CAPACITACIÓN PERSONAL	SISTEMA DE AUDITORÍA INTERNA DE GESTIÓN	POLÍTICAS INTERNAS DE PREVENCIÓN	ASIGNACIÓN CLARA DE RESPONSABILIDADES	EXISTENCIA DE RECUROS HUMANOS SUFICIENTES	EXISTENCIA DE RECUROS TECNOLÓGICOS
RIG-06	Capacitación y disfusión en riesgos							
PST-01	Formulación y aprobación del presupuesto							
PST-02	Ejecución y reforma del presupuesto							
PST-03	Evaluación presupuestaria							
INV-01	Inversiones financieras							
INV-02	Fijación de tasas activas y pasivas							
TES-01	Custodias de títulos valores							
TES-02	Pagos							
TES-03	Caja General							
TES-04	Caja de ventanilla - Apertura y cierre de caja							
TES-05	Caja de ventanilla - Recepción de pagos de cartera							
CTB-01	Registro Contable							
CTB-02	Emisión de estados financieros							
CTB-03	Obligaciones tributarias							
CTB-04	Archivo de contabilidad							
CTB-05	Conciliaciones bancarias							
CTB-06	Pruebas departamentales							
CTB-07	Amortización de créditos internacionales							

Elaboración: María Elena Ochoa **Fuente: BEV**

Como se puede observar en la tabla presentada, los procesos tienen diferente nivel de criticidad en función de la aplicación de variables, entendiendo este caso de que pueden ser afectados de diferente manera por la presencia de diversos tipos de riesgo.

Por ejemplo, el proceso de Capacitación y difusión en riesgos se encuentra en un nivel crítico en relación a la asignación de responsabilidades del personal a cargo, pero se encuentra en un nivel adecuado en el uso de los sistemas de información internos. Como se aprecia, los procesos pueden tener diferentes comportamientos en función de las variables de medición, situación que hace que la medición de riesgos sea complicada ya que demanda de una verdadera visión integral.

3.2.3.1.3 Procesos críticos del área Informática

Por su propia naturaleza, el área de Informática es crítica en la medición del riesgo operacional. Como se observa en las variables utilizadas en el BEV, los sistemas de información y los recursos informáticos son esenciales para evaluar los niveles de criticidad de todos los procesos existentes.

La falta de integración de la información en una plataforma única y especialmente diseñada es una falencia que impide gestionar con eficiencia los servicios, provocando duplicidad en las funciones administrativas.

TABLA No 8

Procesos críticos del área Informática

SUBPROCESO	VARIABLES DE RIESGO OPERACIONAL INTERNO						
	SISTEMA DE NFORMACIÓN	CAPACITACIÓN PERSONAL	SISTEMA DE AUDITORÍA INTERNA DE GESTIÓN	POLÍTICAS INTERNAS DE PREVENCIÓN	ASIGNACIÓN CLARA DE RESPONSABILIDADES	EXISTENCIA DE RECUROS HUMANOS SUFICIENTES	EXISTENCIA DE RECUROS TECNOLÓGICOS
Desarrollo de aplicaciones							
Administración de aplicaciones							
Administración de recursos tecnológicos							
Mantenimiento preventivo							
Mantenimiento correctivo							
Help desk							
Plan de desarrollo tecnológico							
Plan de contingencia y continuidad							
Generación de estándares, políticas y manuales							
Capacitación informática							
Ingreso de comunicaciones							
Despacho de comunicaciones							
Archivo central							
Requerimiento de documentos							
Secretaria de cuerpos colegiados, comités o comisiones							

Elaboración: María Elena Ochoa **Fuente: BEV**

Los riesgos son visibles en los procesos de Informática en el cuadro presentado, situación que no solo afecta los procesos presentados sino a toda la estructura del BEV. Lamentablemente, el crecimiento organizacional ha generado soluciones parciales que eliminan los efectos pero no las causas, produciendo fallas y poca estandarización que eleva considerablemente el riesgo operativo del BEV.

3.2.3.1.4 Procesos críticos de las áreas de Negocios y Operaciones

Sus procesos representan la base competitiva del BEV y establecen los requerimientos necesarios para poder atender las necesidades de sus clientes. Esta condición hace que cualquier evento que se desvíe de su comportamiento normal de calidad establecido, afecte considerablemente el rendimiento de toda el negocio, situación que fácilmente puede ser percibida por el cliente ya que se encuentra inmerso en la mayoría de las actividades existentes.

El nivel de criticidad del riesgo establecido, se detalla en la siguiente tabla:

TABLA No 9

Procesos Críticos de las áreas de Negocios y Operaciones

(Ver siguiente página)

	VARIABLES DE RIESGO OPERACIONAL INTERNO						
SUBPROCESO	SISTEMA DE NFORMACIÓN	CAPACITACIÓN PERSONAL	SISTEMA DE AUDITORÍA INTERNA DE GESTIÓN	POLÍTICAS INTERNAS DE PREVENCIÓN	ASIGNACIÓN CLARA DE RESPONSABILIDADES	EXISTENCIA DE RECUROS HUMANOS SUFICIENTES	EXISTENCIA DE RECUROS TECNOLÓGICOS
Registro Contable de tranferencia de cartera de Fideicomisos inmobiliarios inegrales							
Registro Contable de cartera de arrastre							
Pagos de Cartera							
Pago de Cartera de Agencias Cerradas							
Pago de Cartera mediante Banco del Pichincha							
Pagos de Cartera mediante SERVIPAGOS							
Pagos de Cartera mediante SERVIPAGOS Contingente							
Recuperación extrajudicial de cartera							
Recuperación judicial de cartera							
Castigo de cartera y recuperación							
Reestructuración de Operaciones Crediticias Vencidas Y Castigadas.							
Aperturas de cuentas de ahorro							
Depósitos							
Retiros y cancelación de libretas de ahorro							
Emisión de notas de débito y crédito							
Apertura de cuentas de fondos en garantía							
Depósitos de fondos de garantía							
Devolución de fondos en garantía							

Elaboración: María Elena Ochoa **Fuente: BEV**

3.2.3.1.5 Procesos críticos de otros departamentos

Dentro de los procesos que conforman los otros departamentos, es necesario resaltar la importancia que tienen aquellos relacionados con el recurso humano. Debido a su alta participación el riesgo de error es sumamente alto y este aumenta cuando no está bien definido, es decir, que sus competencias no se encuentran acorde a las necesidades de sus responsabilidades.

Otro factor que afecta su comportamiento es el nivel de formación y preparación que el personal a cargo de las diferentes funciones. Por esta razón se ha decidido separar los procesos de Recursos Humanos en una tabla independiente para posteriormente evaluar los procesos necesarios para minimizar su riesgo.

TABLA No 10

Procesos críticos de Recursos Humanos

		VARIABLES DE RIESGO OPERACIONAL INTERNO						
CODIFICACION	SUBPROCESO	SISTEMA DE NFORMACIÓN	CAPACITACIÓN PERSONAL	SISTEMA DE AUDITORÍA INTERNA DE GESTIÓN	POLÍTICAS INTERNAS DE PREVENCIÓN	ASIGNACIÓN CLARA DE RESPONSABILIDADES	EXISTENCIA DE RECUROS HUMANOS SUFICIENTES	EXISTENCIA DE RECUROS TECNOLÓGICOS
RHH-01	Planificación de RRHH							
RHH-02	Reclutamiento y selección							
RHH-03	Incorporación							
RHH-04	Contratación							
RHH-05	Inducción							
RHH-06	Capacitación							
RHH-07	Evaluación del desempeño							
RHH-08	Entorno y clima organizacional							
RHH-09	Nómina							
RHH-10	Beneficios sociales							
RHH-11	Registro contable							
RHH-12	Comisiones de servicio							
RHH-13	Desvinculaciones							
RHH-14	Moviomiento de personal							

Elaboración: María Elena Ochoa **Fuente: BEV**

A continuación el análisis de los procesos de otros departamentos, en donde se detallan los diferentes subprocesos:

TABLA No 11

Procesos críticos de otros departamentos

		VARIABLES DE RIESGO OPERACIONAL INTERNO						
CODIFICACION	SUBPROCESO	SISTEMA DE NFORMACIÓN	CAPACITACIÓN PERSONAL	SISTEMA DE AUDITORÍA INTERNA DE GESTIÓN	POLÍTICAS INTERNAS DE PREVENCIÓN	ASIGNACIÓN CLARA DE RESPONSABILIDADES	EXISTENCIA DE RECUROS HUMANOS SUFICIENTES	EXISTENCIA DE RECUROS TECNOLÓGICOS
PLN-01	Planificación Estratégica							
PLN-02	Planificación Operativa							
PLN-03	Seguimiento de Planes							
NOR-01	Generación de la Normativa Institucional							
CTR-01	Control de Gestión							
DOR-01	Elaboración y actualización de procedimientos							
DOR-02	Auditoría de procesos							
ADM-01	Adquisiciones							
ADM-02	Calificación de Proveedores							
ADM-03	Inventarios, proveeduría y bodega							
ADM-04	Egresos de bienes							
ADM-05	Registro contable área administrativa							
ADM-06	Seguridad							
ADM-07	Administración de Vehículos							
ADM-08	Mantenimiento de vehículos							
ADM-09	Mantenimiento de edificios							
ADM-10	Mantenimiento Generador eléctrico							
ADM-11	Formulación, Ejecución y evaluación presupuestaria de gastos operativos área administrativa							
ADM-12	Venta de bienes de arrastre							
ADM-11	Enajenación de bienes improductivos							
SMD-01	Medicina general							
SMD-02	Odontología							
SMD-03	Fisioterapia							
SMD-04	Medicina preventiva							
SMD-05	Provisión medicamentos e insumos							
SEG-01	Contratación de seguros							
SEG-02	Gestión de seguros							
SEG-03	Contabilidad de seguros							
ASJ-01	Asesoría y consultoría jurídica							
ASJ-02	Elaboración y actualización de la normativa institucional							
ASJ-03	Informes jurídicos de calificación para operaciones de negocios							
ASJ-04	Patrocinio legal							
ASJ-05	Contratación							
ASJ-06	Escrituración micro							
ASJ-07	Escrituración macro							
ASJ-08	Cancelación de hipotecas y rectificaciones							
ASJ-09	Lavantamiento de patrimonia familiar							
RIG-01	Creación de metodologías y políticas							
RIG-02	Identificación de riesgo							
RIG-03	Medición de riesgo							
RIG-04	Control y mitigación de riesgos							
RIG-05	Seguimiento de riesgos							
VTA-01	Enajenación de bienes improductivos							
VTA-02	Venta de bienes de arrastre							
CSO-01	Producción y difusión de información							
AIT-01	Planificación de auditoría							
AIT-02	Ejecución de auditoría							
AIT-03	Evaluación							
AIT-04	Seguimiento							

Elaboración: María Elena Ochoa **Fuente: BEV**

3.2.4 Estadísticas generales del nivel de riesgo operacional de los procesos

Identificado el nivel de riesgo operacional actual de los diferentes procesos del BEV, se ha procedido a analizar estadísticamente los datos existentes con el objetivo de examinar el estado general de la institución.

Se obtuvieron los siguientes resultados:

TABLA No 12

Resumen de cuadros estadísticos de riesgo BEV

				OTROS DEPARTAMENTOS			
	ÁREA FINANCIERA	ÁREA INFORMÁTICA	ÁREA DE NEGOCIOS	RRHH	OTROS	TOTAL	%
	13	19	18	26	65	141	17,94
	36	46	31	23	165	301	38,30
	57	29	55	27	53	221	28,12
	18	10	21	22	52	123	15,65
					TOTAL	786	100,00

Elaboración: María Elena Ochoa

Los cuadros estadísticos desarrollados muestran un comportamiento moderado predominante, permitiendo establecer las áreas críticas que actualmente pueden afectar el normal desarrollo de las actividades del BEV y que serán la base para la propuesta a elaborar.

3.2.4.1 Área Financiera

TABLA No 13

Cuadros estadísticos de riesgo BEV -área Financiera-

	ÁREA FINANCIERA	%
	13	10,48
	36	29,03
	57	45,97
	18	14,52
TOTAL	**124**	**100,00**

Elaboración: María Elena Ochoa

La concentración de los procesos en el área Financiera se encuentran en amarillo, lo que implica que si bien es cierto presentan un peligro eminente, han sido afectados levemente, situación que debe ser revisada a fin de evitar daños de mayor magnitud.

3.2.4.2 Área Informática

TABLA No 14

Cuadros estadísticos de riesgo BEV-área Informática-

	ÁREA DE INFORMÁTICA	%
	20	13,07
	43	28,10
	63	41,18
	27	17,65
TOTAL	153	100,00

Elaboración: María Elena Ochoa

El área de Informática tiene una importante concentración de sus procesos en riesgo bajo y moderado situación que evidencia de que existen variables que están incidiendo negativamente en su desarrollo. Es importante señalar que el 17,65% de sus procesos se encuentran afectados.

3.2.4.3 Área de Negocios

TABLA No 15

Cuadros estadísticos de riesgo BEV -área de Negocios-

	ÁREA DE NEGOCIOS	%
	18	14,40
	31	24,80
	55	44,00
	21	16,80
TOTAL	125	100,00

Elaboración: María Elena Ochoa

El área de Negocios, mantiene una tendencia estable con respecto a todos los procesos del BEV. Dentro de esta área, el riesgo más común se encuentra en un nivel moderado, no obstante la cantidad de riesgo alto es considerable y debe provocar acciones inmediatas.

3.2.4.4 Otros departamentos

TABLA No 16

Cuadros estadísticos de riesgo BEV – otros departamentos -

	OTROS DEPARTAMENTOS			
	RRHH	OTROS	TOTAL	TASA
	26	65	91	21,02
	23	165	188	43,42
	27	53	80	18,48
	22	52	74	17,09
TOTAL	98	335	433	100,00

Elaboración: María Elena Ochoa

Como se observa, si bien es cierto predominan los procesos con riesgo bajo, existe una tasa importante de procesos en alto riesgo, por lo que es necesario desarrollar planes en forma urgente que permitan su inmediata atención.

4. PROPUESTA METODOLÓGICA PARA LA ELABORACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO

4.1 ALCANCE DEL PLAN DE CONTINUIDAD DEL NEGOCIO

El plan de continuidad del negocio es un sistema diseñado para reducir riesgos y pérdidas económicas ante la interrupción inesperada de procesos de muy alta criticidad de la institución, ya que para otros bastará el desarrollo de planes de contingencia, de acuerdo a lo establecido en la Resolución de Riesgo Operativo, de la Superintendencia de Bancos JB-2005-834.

El propósito del establecimiento del plan de continuidad del negocio es el de proporcionar procedimientos para mantener las operaciones esenciales del negocio después de que ha sucedido un evento que puede afectar directamente los objetivos de la institución.

El plan de continuidad del negocio tiene el siguiente alcance y definición:

- La cobertura del plan de continuidad del negocio será efectuada para las siguientes áreas:
    - Oficinas Centrales del BEV
    - Sucursales a nivel nacional del BEV
    - Centro de Datos
    - Departamentos de la institución
- El plan de continuidad del negocio se lo efectuará para los siguientes tipos de incidentes que se puedan presentar:
    - Aquellos que causen daño físico tanto a las instalaciones como a los equipos que este contenga.
    - Los que afecten de manera directa o indirecta al acceso a las instalaciones.

- Desastres naturales
- Cualquier incidente externo o interno que pueda causar paralización en las actividades normales.
- Incidentes que afecten los datos e información de la institución
- Incidentes que pongan en peligro la vida de las personas tanto colaboradores como usuarios y clientes.

4.2. DESCRIPCIÓN DE LAS FASES DE LA METODOLOGÍA PROPUESTA

Para la elaboración del plan de continuidad del negocio aplicable al BEV, el presente capítulo ha desarrollado una metodología basada en fases de cumplimiento, las mismas que tienen como fin una eficiente prevención, corrección y recuperación de daños que puedan ser causados por eventos internos o externos.

La metodología propuesta está conformada por ocho fases, que se muestran en la siguiente ilustración:

GRAFICO No 6

Fases de desarrollo de la metodología para la elaboración de un plan de continuidad

		RESPONSABLES
FASE I	PLANIFICACIÓN DEL PROYECTO	SUBGERENTES ADMINISTRATIVO, RIESGOS
FASE II	LEVANTAMIENTO DE PROCESOS (MAPEO)	SUBGERENTE DE RECURSOS HUMANOS
FASE III	ANÁLISIS DE RIESGOS (RA)	SUBGERENTE DE RIESGOS
FASE IV	ANÁLISIS DEL IMPACTO DEL NEGOCIO (BIA)	SUBGERENTES DE RIESGOS, FINANCIERO RECURSOS HUMANOS, TECNOLOGÍA
FASE V	DISEÑO DE ESTRATEGIAS	SUBGERENTES DE RIESGOS, RECURSOS HUMANOS, TECNOLOGÍA
FASE VI	CAPACITACIÓN Y COMUNICACIÓN	PRESIDENTE Y CORDINADOR DEL COMITÉ, JEFE DE COMUNICACIÓN
FASE VII	PRUEBAS	COORDINADOR DEL COMITÉ, SUBGERENTES DE RIESGOS, RECURSOS HUMANOS, TECNOLOGÍA
FASE VIII	MANTENIMIENTO Y ACTUALIZACIÓN	COORDINADOR DEL COMITÉ, SUBGERENTES DE RIESGOS, TECNOLOGÍA

Elaboración: María Elena Ochoa

4.2.1 Planificación del proyecto:

Para que el plan de continuidad del negocio tenga un efecto positivo en el BEV y sea aplicado adecuadamente es necesario definir un compromiso que permita ejecutar su implementación.

De esta manera, se entiende como planificación del proyecto al conjunto de acciones necesarias para justificar la validez del mismo a los niveles gerenciales de la institución. Los responsables encargados de efectuar esta fase son el Subgerente Bancario Administrativo y el Subgerente Bancario de Riesgos.

La obtención de apoyo es fundamental para su aplicación y principalmente para la generación de beneficios a la institución, relacionados con el objetivo de minimizar los impactos que afecten el normal desenvolvimiento de las actividades y el desempeño de los recursos asignados.

De igual manera, la planificación del proyecto está enfocada en evitar que los procesos sean interrumpidos generando costos innecesarios a la institución y reduciendo la calidad de servicio a los diferentes usuarios y colaboradores de la misma.

Es muy importante que dentro de la planificación del plan de continuidad del negocio se establezcan con claridad las metas y objetivos que se espera alcanzar y que los mecanismos sean definidos de manera clara, precisa y concreta.

La metodología planteada dentro de la planificación del proyecto incluye los siguientes cumplimientos:

- Incorporar a la estructura orgánica administrativa un Comité Directivo de Continuidad y Contingencia, que será responsable de la implementación, monitoreo y control del plan.
- Definir y asignar las responsabilidades al personal perteneciente al Comité Directivo de Continuidad y Contingencia.

- Establecer brigadas de trabajo en todas las áreas de la institución que apoyen a la ejecución correcta del plan en el caso de presentarse situaciones que afecten el desarrollo eficiente de las actividades.

4.2.2 Levantamiento de procesos (mapeo)

Es necesario conocer los diferentes procesos existentes en el BEV, para poder gestionar adecuadamente el plan de continuidad del negocio orientado específicamente a las amenazas que se puedan presentar, de esta responsabilidad se encargará el Subgerente de Recursos Humanos. Para ello, la metodología plantea los siguientes levantamientos:

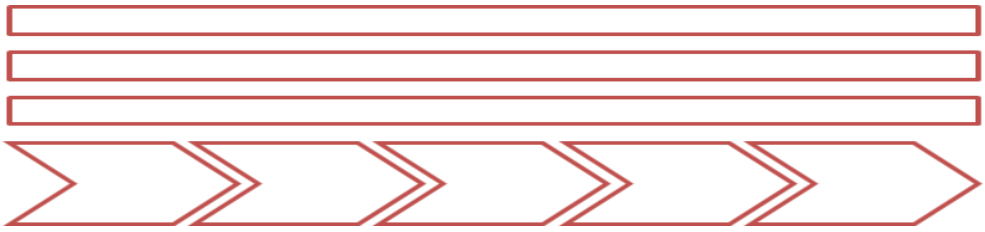
- Levantamiento de los Macro procesos.
- Levantamiento de las actividades de cada proceso.
- Establecimiento de la cadena de valor
- Levantamiento de los recursos que utilizan los procesos.
- Levantamiento de los documentos que utilizan los procesos.
- Levantamiento de los sistemas informáticos utilizados en cada proceso.

4.2.2.1 Levantamiento de los macro procesos

Para el levantamiento de los macro procesos se ha planteado la utilización de la herramienta establecida por Michael Porter en el libro Ventajas Competitivas que se detalla a continuación:

GRAFICO No 7

Levantamiento de macro procesos



Elaboración: María Elena Ochoa

4.2.2.2 Levantamiento de las actividades de cada proceso

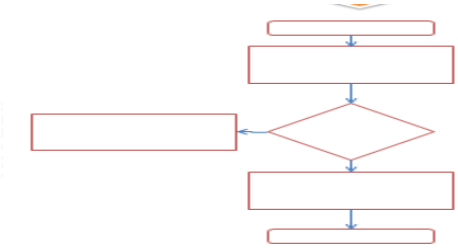
Para el levantamiento de los procesos, se utilizará la técnica de flujogramas que permite identificar paralelamente la siguiente información:

- Descripción de las actividades requeridas para su cumplimiento
- Descripción de las relaciones entre las actividades
- Descripción de los puntos de decisión del proceso
- Descripción de los responsables de las diferentes actividades

El resultado final del levantamiento de las actividades quedará establecido conforme lo indica la siguiente ilustración:

GRAFICO No 8

Diagrama de flujo



Elaboración: María Elena Ochoa

4.2.2.3 Establecimiento de la cadena de valor del negocio

Porter (1987) define la cadena de valor del negocio como: "Una forma de análisis de la actividad empresarial mediante la cual descomponemos una empresa en sus partes constitutivas, buscando identificar fuentes de ventaja competitiva en aquellas actividades generadoras de valor." Esa ventaja competitiva se logra cuando la empresa desarrolla e integra las actividades de su cadena de valor de forma menos costosa y mejor diferenciada.

En este paso la institución deberá establecer todos sus procesos generadores de valor agregado y los márgenes que éstos aportan, para de esta manera determinar los procesos críticos para el negocio.

4.2.2.4 Levantamiento de los recursos que utilizan los procesos

Es muy importante definir qué recursos utilizan los procesos levantados, este levantamiento representa una actualización del inventario, mismo que debe ser clasificado en categorías que permitan disponer de un claro conocimiento para definir el plan de continuidad.

El levantamiento de los recursos se efectuará en base a las siguientes clasificaciones:

- Inventario de equipos informáticos
- Inventario de equipos de comunicación
- Inventario de bienes muebles
- Inventario de suministros de oficina, limpieza, otros

Los inventarios desarrollados permitirán cuantificar los bienes existentes, permitiendo entender la magnitud de daños que agentes internos o externos puedan causar si se presentan.

4.2.2.5 Levantamiento de los documentos que utilizan los procesos

Definir la documentación utilizada es importante para entender el grado de automatización de los mismos. Para ello debe levantarse la documentación para cada una de las actividades existentes en los respectivos procesos.

Para tal efecto, la presente metodología plantea la utilización del siguiente formulario:

TABLA No 17

Formulario para el levantamiento de la documentación utilizada en los procesos

PROCESO:

ACTIVIDAD	DOCUMENTO

Elaboración: María Elena Ochoa

Después de terminar este levantamiento es necesario se disponga de una copia digital de los diferentes documentos utilizados a fin de poder identificarlos con claridad.

4.2.2.6 Levantamiento de los sistemas informáticos utilizados en el proceso

Es importante identificar y reconocer los sistemas informáticos que participan en el desarrollo de los diferentes procesos. En este caso a diferencia de los documentos, el levantamiento puede realizarse por procesos y no por actividades, para lo cual se ha desarrollado el siguiente formulario:

TABLA No 18

Levantamiento de los sistemas informáticos participantes en los procesos

CÓDIGO	PROCESO	SISTEMAS	OBSERVACIONES

Elaboración: María Elena Ochoa

4.2.2.7 Selección de los procesos aplicables para el plan de continuidad del negocio

Una vez conocidos los diferentes procesos participantes en el BEV, es necesario seleccionar aquellos que deberán ser parte del plan de continuidad del negocio, para ello se deberá clasificarlos en función de los siguientes parámetros:

- Definir los procesos que efectivamente disponen de un plan de continuidad del negocio
- Definir los procesos que requieren plan de continuidad del negocio y no han sido incluidos

4.2.2.7.1 Definir los procesos que efectivamente disponen de un plan de continuidad del negocio

Es necesario verificar los procesos que en la actualidad disponen de un plan de continuidad del negocio elaborado, verificando los siguientes puntos:

- Vigencia del plan de continuidad del negocio existente
- Aplicabilidad del plan de continuidad del negocio existente
- Detalles históricos de la aplicación del plan
- Verificación de los resultados en el caso de haber sido aplicado el plan

Es importante dentro de este levantamiento, determinar si el plan de continuidad del negocio ha sido implementado y si este reúne las características técnicas que garanticen efectividad en la prevención, corrección y recuperación de los impactos posibles a presentarse en el mismo.

4.2.2.7.2 Definir los procesos que requieren plan de continuidad del negocio y no han sido incluidos

Dentro de la revisión realizada se identificarán aquellos procesos considerados como críticos que pueden estar amenazados por factores internos y/o externos y que en la actualidad no disponen de ningún plan de continuidad del negocio desarrollado.

Se llama proceso critico al "proceso considerado indispensable para la continuidad de las operaciones y servicios de la entidad, y cuya falta o ejecución deficiente puede producir daño a la imagen institucional o tener un impacto financiero significativo para la organización." [11]

En este caso, los procesos críticos son los que deben ser atendidos con prioridad ya que pueden generar impactos al normal desenvolvimiento de las actividades.

4.2.3 Análisis de riesgos (RA)

"Estudio de las amenazas a que están sometidos los activos de una organización y evaluación de su vulnerabilidad." [12]

La metodología desarrollada aplicada por la Subgerencia de Riesgos, en el campo de análisis de riesgos se enfoca en los siguientes aspectos:

- Amenazas posibles a presentarse
- Vulnerabilidad de los procesos en la presencia de las amenazas posibles
- Probabilidad de ocurrencia de las amenazas detalladas
- Riesgos existentes a los que se expone cada uno de los procesos

---

[11] Juan Gaspar Martínez, *El Plan de Continuidad* de Negocio, *Guía Práctica para su elaboración*, editorial Díaz de Santos, Madrid, España, 2007, p.189.

[12] Juan Gaspar Martínez, *El Plan de Continuidad de Negocio, Guía Práctica para su elaboración*, p.189.

El estudio de los riesgos debe ser completo, debiendo identificarse una serie de aspectos que miden su impacto dentro del BEV. Estos aspectos se pueden clasificar de la siguiente manera:

- Entendimiento de las potenciales pérdidas a presentarse en el BEV
- Identificación de la efectividad de los controles generados

Para el levantamiento del análisis de riesgos se empleará el siguiente formulario:

TABLA No 19

Levantamiento del análisis de riesgos

AMENAZAS	PROBABILIDAD	IMPACTO	PxI	CONTROL

Elaboración: María Elena Ochoa

4.2.3.1 Causas más comunes que generan riesgos en los procesos

Es posible identificar causas comunes de la presencia de los riesgos que facilitan su identificación, en este sentido se citan las más comunes:

- Error Humano
- Fallas en el sistema informático
- Fallas en la infraestructura
- Desastres Naturales

4.2.3.2 Proceso de identificación de riesgos (RA)

4.2.3.2.1 Clasificación del riesgo:

El riesgo se identifica como el conjunto de elementos no controlables que generan impacto al normal desenvolvimiento de las diferentes actividades, procesos y macro procesos.

La presencia de los riesgos es siempre nociva por lo que su oportuno conocimiento e identificación es la base para evitar su presencia.

La clasificación del riesgo, se conforma en base a dos tipos:

- Riesgo interno
- Riesgo externo

4.2.3.2.1.1 Riesgo interno

Se denomina riesgo interno aquel que se genera en función de las propias actividades de la empresa. Es decir, se da producto a posibles fallas que inciden en el comportamiento de las actividades.

El riesgo interno puede ser controlado y evitado, el modelo busca identificarlo oportunamente para evitar su ocurrencia.

Debido a que muchos factores no pueden ser controlados en su totalidad, la identificación del riesgo permite además aplicar correctivos inmediatos que minimizan los daños posibles a presentarse.

Los riesgos internos pueden ser:

a) **Riesgo de imagen:** es la probabilidad de que se forme una opinión pública negativa sobre el servicio bancario prestado.
   La principal causa por las que se origina este riesgo es la pérdida de credibilidad de la institución.

b) **Riesgo gremial:** es la probabilidad de que la institución pueda presentar pérdidas debido a los conflictos que pueda tener con sus empleados.

c) **Riesgo legal:** es el riesgo que surge del incumplimiento de leyes, reglas y prácticas, este riesgo puede ocasionar que los clientes no sean correctamente atendidos e informados sobre sus derechos y obligaciones.

4.2.3.2.1.2 Riesgo externo:

El riesgo externo se presenta por situaciones ajenas a la actividad de la empresa pero que su ocurrencia puede generar diferente tipo de afecciones.

La gravedad del riesgo externo es que tiene múltiples causas por lo que su identificación es más complicada, situación que eleva las posibilidades de impacto negativo en los procesos.

Al igual que el riesgo interno, el modelo desarrollado busca su identificación con el objetivo de establecer planes que actúen inmediatamente eliminando sus causas y efectos.

Los riesgos externos pueden presentarse de diversas formas, para lo cual se establecen las siguientes guías que facilitarán su identificación:

a) Riesgo económico:

El riesgo económico se origina por medidas económicas tomadas por los gobiernos de turno que pueden incidir en los procesos y actividades de la institución.

- **Riesgo internacional:**

  Responde a medidas internacionales que pueden afectar al mercado nacional y por ende cambiar los comportamientos y patrones de la población. Su incidencia puede incentivar o reducir la demanda de esta hacia los servicios y productos que comercializa el BEV afectando sus resultados.

  Dependiendo de las medidas tomadas, las incidencias pueden ser bajas, moderadas o altas.

- **Riesgo nacional:**

  Se enfoca principalmente a medidas económicas tomadas por el gobierno de turno y que pueden al igual que las medidas internacionales incidir en los servicios prestados por el BEV

- **Riesgo sectorial:**

  Las medidas tanto internacionales como nacionales tienen diferente nivel de respuesta en los sectores económicos, situación que dependiendo del impacto pueden incidir en los procesos internos del BEV.

b) Riesgos naturales:

Corresponden a eventos naturales que afectan las actividades internas. Dentro de ellas se citan las más comunes y frecuentes:

- **Erupción volcánica:** En este caso, la ciudad de Quito al encontrarse en el cordón andino de la cordillera de los Andes, se encuentra dentro de una alta probabilidad de ocurrencia.
- **Temblores y terremotos:** Por las mismas razones expuestas en el punto anterior, el nivel de ocurrencia es más alto.
- **Climatológicas:** Dadas por la presencia de cambios drásticos en el clima o la presencia de condiciones que afecten el desarrollo de las actividades ya que aumentan la probabilidad de daños en la infraestructura, medios de comunicación e información.

c) Riesgos políticos:

Es la probabilidad de que un evento político dado resulte en pérdidas para la institución. Existe cuando se percibe una discontinuidad en el ambiente de un país ocasionada por el cambio político, es difícil anticipar las consecuencias que tendrán.

4.2.4 Análisis del impacto del negocio (BIA)

"BIA (*Business Impact Analysis*) es la actividad de la Gestión de la Continuidad del Negocio que identifica las funciones vitales del negocio y sus dependencias. Estas dependencias pueden incluir proveedores, personas, otros procesos de negocio, servicios de Tecnología de la Información, etc. Dichos requerimientos incluyen objetivos de tiempos de recuperación,

objetivos del punto de recuperación y los objetivos de nivel de servicio mínimos para cada Servicio"[13]

El propósito fundamental del análisis de impacto sobre el negocio, conocido más comúnmente como BIA, es determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto. Las Subgerencias que se encargarán de efectuar este análisis son: Riesgos, Financiero, Recursos Humanos y Tecnología.

Para un desarrollo adecuado del plan de continuidad del negocio, es necesario establecer un eficiente análisis del impacto del negocio a fin de identificar los procesos críticos y los activos de información críticos.

En este sentido, es necesario enfocarse en los siguientes aspectos:

- Determinar los impactos cuantitativos y cualitativos de la interrupción
- Determinar el tiempo de recuperación RTO (*Recovery Time Objetive*)
- Determinar el punto objetivo de recuperación RPO (*Recovery Point Objetive*)
- Determinar los controles y estrategias a desarrollar

4.2.4.1 Determinar los impactos cuantitativos y cualitativos de la interrupción

Cada acción que genera un impacto en los diferentes procesos del BEV, puede producir consecuencias negativas, las cuales se miden de manera cuantitativa y/o cualitativa según sea el caso.

Para tal efecto, se debe analizar las interrupciones producidas, las mismas que pueden detallarse conforme a la siguiente manera.

---

[13] ITIL:2007, ITIL V3 Glossary, 30 May 2007, p.4, en http://www.best-management-practice.com/gempdf/ITIL_Glossary_V3_1_24.pdf

a) Medición cuantitativa: se deberá efectuar las siguientes evaluaciones:

- Análisis del tiempo de interrupción de los procesos
- Análisis del costo de interrupción medido por los recursos paralizados.

b) Medición cualitativa:

- Análisis de la pérdida de imagen de la institución por afección en los servicios
- Análisis de los niveles de motivación del personal

4.2.4.2 Determinar el tiempo de recuperación RTO

"El RTO (Recovery Time Objetive) es el periodo de tiempo después de ocurrido el desastre que es necesario para que las funciones básicas del negocio sean restauradas"[14]

Se enfoca principalmente en el análisis del tiempo requerido para poder volver a recuperar la situación normal de funcionamiento del proceso.

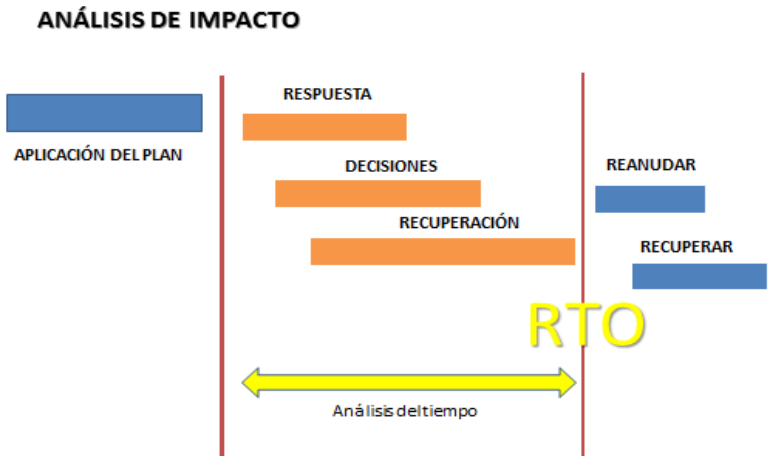
La metodología planteada dispone de procesos con una oportuna respuesta que permitan la recuperación después de sucedido el evento, conforme se detalla en la siguiente ilustración:

GRAFICO No. 9

Tiempo de recuperación RTO

(Ver siguiente página)

[14] Albion Reserch Ltd., *Risky Thinking, Glossary*, 2011, en http://www.riskythinking.com/glossary



Elaboración: María Elena Ochoa

Para el análisis del RTO se utilizará el siguiente formulario:

TABLA No 20

Determinación del Tiempo de Recuperación RTO

	Función/Proceso de Negocio	RTO	Comentarios
1			
2			
3			
4			
5			

Elaborador por: María Elena Ochoa

4.2.4.3 Determinar el punto objetivo de recuperación RPO

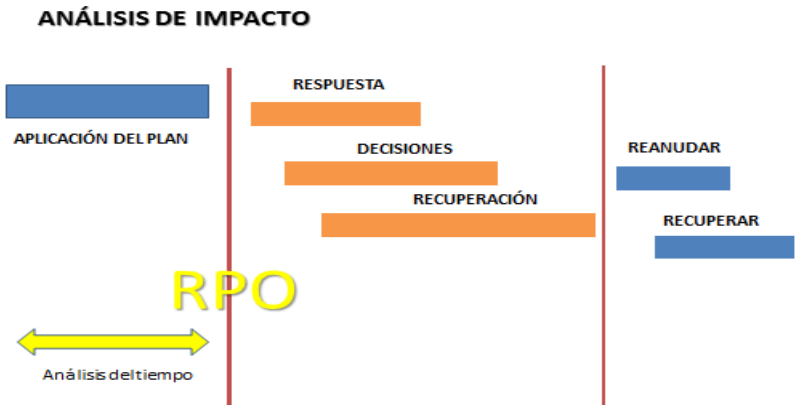
"El RPO (Recovery Point Objetive) es el momento en el que las actividades deben estar recuperadas para comenzar el trabajo después de una interrupción" [15]

[15] The BCI, *Glossary of Business Continuity Management Terms*, 2009, en http://recoveryspecialties.com/glossary.html

Basado en el inicio de la aplicación del plan que permita la eliminación de los impactos generados conforme se detalla en la siguiente ilustración:

GRAFICO No 10

Punto objetivo de recuperación RPO



Elaboración: María Elena Ochoa

Para el análisis de RPO se utilizará el siguiente formulario:

TABLA No 21

Determinación del punto objetivo de recuperación RPO

	Función/Proceso de Negocio	RPO	Comentarios
1			
2			
3			
4			
5			

Elaboración: María Elena Ochoa

El análisis del impacto del negocio (BIA) busca permitir al BEV alcanzar una serie de beneficios que minimicen las interrupciones provocadas por las amenazas posibles a presentarse o a su vez disponer del menor tiempo de recuperación en base a la ágil aplicación del plan desarrollado para eliminar las causas detectadas.

Los beneficios esperados de la aplicación del análisis del impacto se detallan a continuación.

- Reducir la responsabilidad legal
- Minimizar la pérdida económica potencial
- Disminuir la exposición potencial
- Reducir la interrupción de las operaciones normales
- Asegurar la estabilidad de la empresa
- Asegurar una recuperación ordenada
- Minimizar los montos de las primas de seguros
- Reducir la dependencia del personal clave
- Incrementar la protección de los activos
- Garantizar la seguridad del personal y de los usuarios de los servicios del BEV
- Cumplir con las disposiciones legales y regulatorias.

Para un adecuado análisis del impacto se deberá establecer un levantamiento enfocado en los aspectos claves en la evaluación, para lo cual se ha desarrollado el siguiente formulario.

TABLA No 22

Formulario para determinar los aspectos claves de la evaluación

PROCESO _____

IMPACTO _____

CARACTERÍSTICAS

ECONÓMICO	POLÍTICO	SOCIAL	DE IMAGEN	LEGAL	GREMIAL

Elaboración: María Elena Ochoa

Es fundamental que para la determinación de los aspectos claves de la evaluación se tome en consideración a contratistas, proveedores, usuarios, colaboradores en base a todos los procesos levantados.

4.2.5 Diseño de Estrategias

El desarrollo de estrategias se concentra en las acciones que deberán cumplirse para minimizar los impactos determinados y debidamente cuantificados y evaluados. Las Subgerencias que liderarán esta fase son: Riesgos, Recursos Humanos y Tecnología.

En este aspecto, el diseño de estrategias se concentra principalmente en:

4.2.5.1 Respaldar al recurso humano, para lo cual se deberá:

- Identificación clara de los roles, funciones y responsabilidades del recurso humano.
- Conocer las acciones inmediatas a cumplir en el caso de ser activado un plan de continuidad del negocio.
- Conocimiento profundo de las herramientas a utilizar en la aplicación el plan de continuidad del negocio.
- Entendimiento completo de la relación de las actividades de los procesos críticos para una adecuada aplicación del plan.

4.2.5.2 Respaldar el recurso informático, digital y de telecomunicaciones, efectuándose las siguientes estrategias:

- Conocimiento de las necesidades de telecomunicaciones antes, durante y después de la presencia de un impacto.
- Conocimiento de las fuentes de información que deben respaldarse
- Conocimiento del plan de respaldo de la información

Para lo cual la metodología desarrollada contempla la aplicación de las siguientes estrategias:

- Desarrollar procedimientos de recuperación para los procesos críticos existentes en el BEV.
- Desarrollar los procesos de respaldo de la información digital en localidades externas e internas para disponer de varias fuentes paralelas.
- Garantizar una infraestructura que faculte la aplicación de respuestas rápidas y eficientes en conformidad a los planes desarrollados.
- Planificar la recuperación y reanudación de las operaciones afectadas.
- Suscribir los contratos comerciales necesarios para la ejecución de los procedimientos de reanudación y recuperación.
- Suscribir los contratos de seguros en caso de ser requeridos.
- Asignar responsables a cada personal involucrado y área del BEV involucrados en el plan, en: distintas etapas del desastre y en el mantenimiento del plan a lo largo del tiempo.
- Definir acciones complementarias referentes a: la comunicación a clientes y proveedores, distribución física de lugares de trabajo del personal, estrategias de trabajo, otros recursos.

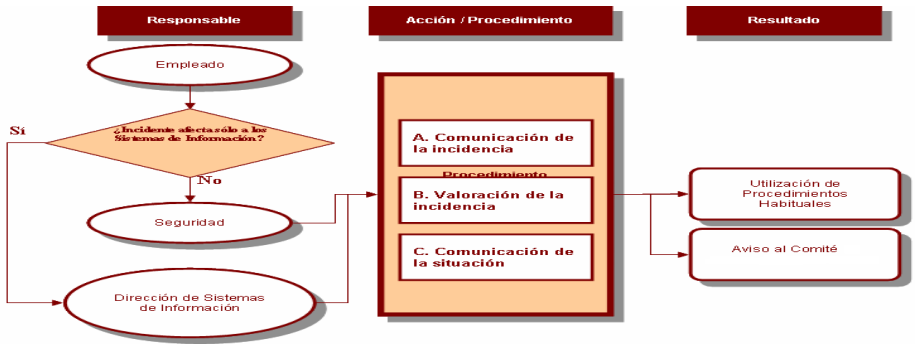
Es muy importante garantizar que las estrategias definidas estén acorde a los objetivos del BEV debiendo en todos los casos permitir que los procesos de negocio puedan restablecerse eficientemente dentro de los plazos fijados y requeridos (RTO).

En este sentido, las estrategias se clasificarán en función de tres tipos de procedimientos que se detallan a continuación

a) **Procedimientos de alerta:** Los responsables de los procesos deberán identificar si el desastre presentado afecta a toda la organización o sólo a los sistemas de información, con este antecedente se determinarán acciones encaminadas a efectuar la valoración del incidente y de ser el caso el aviso al Comité Directivo de Continuidad y Contingencia, más adelante se explicará la conformación y responsabilidades de este cuerpo colegiado.

GRAFICO No 11

Procedimientos de alerta



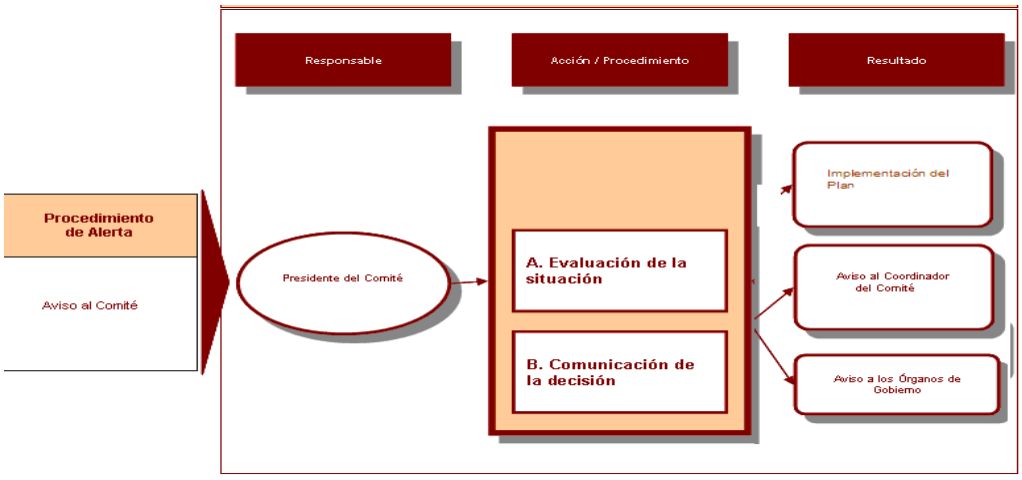
Elaboración: María Elena Ochoa

b) Procedimientos de evaluación: El Comité Directivo de Continuidad y Contingencia evaluará la situación y la comunicará las decisiones, además será el responsable de implementar el plan de continuidad, y de efectuar los avisos necesarios dentro y fuera de la organización.

GRAFICO No 12

Procedimientos de

evaluación



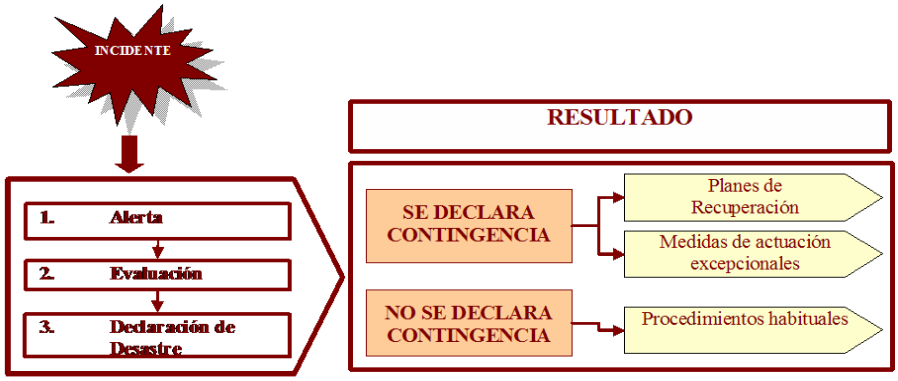
Elaboración: María Elena Ochoa

c) Procedimientos de gestión de crisis: Dentro de este procedimiento se establece el incidente, se crea las alertas y si es necesario se declara el desastre, es ahí en donde se

establecerán los planes de recuperación, a continuación el flujo en donde se detallan los procesos que se llevarán a cabo para la gestión de crisis:

GRAFICO No 13

Procedimientos de gestión de crisis



Elaboración: María Elena Ochoa

Los planes de recuperación, están enfocados a conseguir el restablecimiento de las actividades normales de la institución en base a corregir los daños presentados durante la manifestación de la amenaza, más adelante se explicarán las estrategias a ser aplicadas en este plan.

Para llevar a cabo los planes de continuidad es necesario analizar las formas de dar respuesta a la necesidad de un centro alternativo, que es un "lugar previamente definido en el plan de continuidad del negocio, donde está previsto trasladar las operaciones de tratamiento de la información en el supuesto de que haya imposibilidad de uso de las instalaciones habituales. Debe estar situado a una distancia prudencial de las instalaciones." [16]

El centro alterno permitirá que la institución pueda operar en los tiempos estimados, estos centros pueden ser:

a) **Centro frío:** Es una sala vacía preparada con las condiciones ambientales necesarias

[16] Juan Gaspar Martínez, *El Plan de Continuidad de Negocio, Guía Práctica para su elaboración*, Ediciones Díaz Santos, Madrid, España, 2006, p.191

para albergar equipos informáticos, este centro debe poseer instalaciones de potencia, con climatización, falso suelo y una cierta estructura de comunicaciones. Puede ser una alternativa apropiada para el BEV, pues es recomendable para organizaciones que por su estructura pueden estar un cierto periodo de tiempo sin servicios informáticos funcionando con procedimientos alternativos.

b) **Centro caliente:** Es una instalación con un centro de bases de datos, totalmente configurado a las especificaciones del cliente y disponible en pocas horas, está recomendado para organizaciones en las cuales su umbral de recuperación no supera las 24 o 48 horas.

c) **Centro espejo:** Es utilizado en el caso de las necesidades de respuesta inmediatas, consiste en dos instalaciones idénticas y actualizadas permanentemente con el objetivo de que una de ellas se haga cargo automáticamente del trabajo si la otra sufre una interrupción.

d) **Centro móvil:** Es una sala acondicionada, equipada en un contenedor y configurable en pocas horas, dependiendo del centro de suministro los umbrales de recuperación cubiertos pueden ir desde 6-8 horas en adelante.

4.2.6 Capacitación y comunicación

Para la implementación del plan de continuidad del negocio es fundamental que todos los empleados del BEV tengan un claro conocimiento de los riesgos existentes, las amenazas posibles a presentarse y su participación dentro de los procedimientos a ejecutarse.

La adecuada capacitación permitirá la pronta y eficiente ejecución de los mismos, lo que hará que se minimicen los impactos posibles a presentarse en función de las amenazas ocurridas.

La concientización del empleado es requerida para que se puedan obtener los beneficios planteados del plan, para lo cual es fundamental que conozca la manera efectiva de la aplicación de un plan, así como también sus procedimientos y responsabilidades a fin de que sea

correctamente implementado.

La presente metodología, recomienda de esta manera seguir el siguiente procedimiento:

- Recordar las prácticas básicas de seguridad
- Identificar con claridad las vulnerabilidades y los planes que las minimizan
- Incorporar a todo el personal en la aplicación de los planes de continuidad del negocio. Dentro de la incorporación deberá involucrarse a los nuevos colaboradores permanentemente.
- Realizar las prácticas o simulacros requeridos a fin de que el personal identifique su participación en la aplicación.
- La capacitación deberá necesariamente incluir a usuarios y proveedores así como también contratistas.

Para una correcta aplicación de los programas de capacitación y comunicación se sugiere utilizar material impreso y digital a fin de que siempre se encuentre visible y disponible al usuario. De igual manera, como se indicó anteriormente es fundamental el desarrollo de simulacros a fin de que el personal conozca claramente su participación y principalmente la importancia de los planes desarrollados tanto para la institución como para el personal de todo el BEV.

En este sentido, la presente metodología propone la realización de campañas identificadas que sean de conocimiento general de todos los involucrados, proceso que también debe ser evaluado para que los niveles alcanzados sean óptimos y brinden garantías en su aplicación.

4.2.7 Pruebas

Es necesario someter el plan a pruebas y ejercicios para asegurar que se operacional; los planes deben ser probados periódicamente para garantizar que están actualizados, que son eficaces y que todos los miembros del equipo de recuperación y demás personal los conoce.

Las pruebas pueden ser: estáticas, dinámicas y funcionales.

Las pruebas estáticas, sirven para determinar que los equipos necesarios están en el lugar determinado previamente.

Las pruebas dinámicas, establecen que el equipo cumple los requerimientos operacionales.

Las pruebas funcionales, sirven para determinar si los procedimientos a ser establecidos son los correctos.

Las pruebas deben ser permanentes, orientadas a la solución de temas reales, deben ir aumentando en grado de complejidad, ser documentadas y analizadas.

4.2.8 Mantenimiento y actualización

Debido al constante cambio de los procesos producto al avance científico y tecnológico y al nacimiento de nuevas amenazas principalmente relacionados con estos aspectos, es importante que el plan de continuidad del negocio permanezca siempre actualizado acorde a las necesidades de la institución.

Es necesario que se efectúen revisiones periódicas que determinen la validez en la aplicación de los planes de continuidad, promoviendo permanentemente actualizaciones que garanticen que se encuentran totalmente vigentes y ejecutables en base a la realidad del BEV y acorde a las amenazas tanto internas como externas posibles de presentarse.

Como es comprensible la revisión debe efectuarse en función de los posibles cambios principalmente en los siguientes elementos participantes:

- Personal
- Direcciones, números telefónicos del personal
- Estrategia de los negocios

- Ubicación, instalaciones y recursos

Para un adecuado mantenimiento del plan de continuidad del negocio, la presente metodología plantea cuatro áreas de ejecución que se detallan en la siguiente ilustración:

GRAFICO No 14

Gestión del mantenimiento y actualización del plan de continuidad del negocio

Elaboración: María Elena Ochoa

4.2.8.1 Pruebas y activaciones

Todo plan de continuidad del negocio necesita de la respectiva calibración, representando esta los ajustes necesarios para que pueda ser ejecutado de manera adecuada. Las pruebas se relacionan a ejercicios que el personal cumple con el objetivo de conocer los procedimientos, sus responsabilidades y la manera de interacción con otras personas o recursos.

La activación del plan se da cuando las pruebas han alcanzado un desarrollo oportuno y disponen de un nivel apto para poder ser implementado, contando con las suficientes garantías para alcanzar los beneficios citados.

4.2.8.2 Revisión y actualización

Todo plan de continuidad del negocio deberá ser permanentemente monitoreado a fin de que sus acciones estén acorde a la realidad y necesidad del BEV en total conformidad a las posibles amenazas y riesgos que se puedan presentar.

La actualización se basa en hacer que las acciones y actividades sean modificadas si el caso lo requiere, con el objetivo que su ejecución permita brindar todas las garantías necesarias.

Es importante señalar que la revisión y actualización del plan de continuidad del negocio es un proceso continuo para lo cual se deberán establecer equipos pertinentes que ejecuten esta responsabilidad.

4.2.8.3 Concientización y capacitación

La concientización establece la comprensión de la importancia que tiene el plan de continuidad del negocio para el BEV, para ello se deberá solicitar a todo el personal su adecuada aplicación, situación que demanda a su vez de procesos de capacitación.

Los programas de capacitación son necesarios para que el personal tenga clara su participación e incidencia dentro del plan. De igual manera, brinda un amplio conocimiento sobre los efectos que tienen dentro del BEV, enfocándose en los beneficios que produce para todos los recursos involucrados.

Para desarrollarse adecuadamente deberá establecer cronogramas de capacitación, basados en temas puntuales con la participación de todo el personal debidamente clasificado en función de sus responsabilidades.

Como se mencionó anteriormente, los programas de capacitación deberán ser respaldados con material impreso estratégicamente ubicado y distribuido a fin de que siempre esté al alcance de los involucrados.

4.2.8.4 Cambios en el BEV

Si es necesario, deberán establecerse cambios en los diferentes procesos existentes dentro del BEV, conforme a una política de mejoramiento continuo y en busca de mejores alternativas para minimizar las amenazas posibles a presentarse y de esta manera evitar interrupciones que generen riesgos y pérdidas a la institución.

La metodología planteada abarca ocho fases, cada una de ellas importantes para construir un adecuado plan de continuidad del negocio, enfocado a minimizar los impactos producidos por la presencia de amenazas que alteren el normal funcionamiento y desempeño de las diferentes actividades.

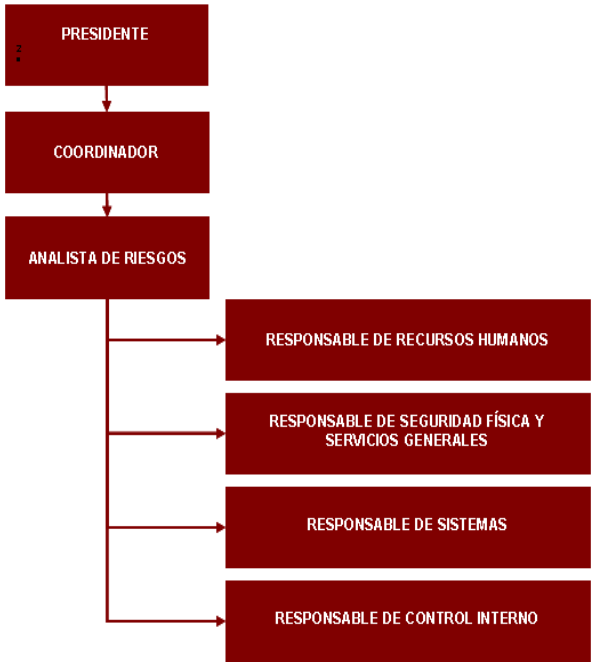
Es importante que se establezcan las aprobaciones requeridas para que su ejecución sea eficiente y permita beneficiar al BEV.

4.3. CONFORMACIÓN DEL COMITÉ DIRECTIVO DE CONTINUIDAD Y CONTINGENCIA

En la siguiente ilustración se detalla la conformación del Comité Directivo de Continuidad y Contingencia:

GRAFICO No 15

Estructura del Comité Directivo de Continuidad y Contingencia



Elaboración: María Elena Ochoa

Para la incorporación del Comité Directivo de Continuidad y Contingencia, se establecen las siguientes funciones:

a) **Presidente:** deberá ser la máxima autoridad de la institución, ya que este tendrá el poder de decisión. Dentro de las funciones del presidente se encuentran las siguientes:

- Controlar la ejecución del plan de continuidad del negocio.
- Monitorear el adecuado uso de los recursos presupuestados en base a la ocurrencia de un evento
- Aprobar los cambios y ajustes requeridos dentro de la aplicación del plan de continuidad del negocio
- Ser la voz informativa sobre las respuestas que la institución ha establecido para el manejo de incidentes.
- Ser el responsable de establecer el protocolo de notificación oficial ante la ocurrencia de un desastre.

b) **Coordinador:** Se encargará de:

- Llevar a cabo las decisiones tomadas por el Comité Directivo de Continuidad y Contingencia
- Documentar los manuales de continuidad de la institución
- Actualizar los manuales de continuidad.
- Establecer las pruebas requeridas para la implementación adecuada del plan de continuidad del negocio.
- Llevar un control adecuado de la actualización de: procesos, recursos humanos, recursos tecnológicos, inventarios físicos.
- Activación del personal de soporte y equipos responsables de los departamentos.

c) **Analista de riesgos:** El avance de la tecnología y la administración genera también la ocurrencia de nuevas amenazas que deben ser determinadas con anticipación para la incorporación de planes que minimicen sus efectos. Para ello, el analista de riesgos perteneciente al comité planteado deberá cumplir las siguientes responsabilidades.

- Verificar la existencia de riesgos tanto internos como externos que puedan afectar al normal desempeño de las actividades.

- Incorporar el plan de continuidad necesario en función de los riesgos detectados
- Coordinar la capacitación del plan de continuidad a las brigadas de apoyo.

d) Responsables de los diferentes departamentos clave: Los responsables de las diferentes áreas lo conforman el personal de los departamentos clave del BEV organizados y debidamente capacitados para la ejecución del plan de continuidad del negocio. Para un mayor control en su cumplimiento, cada responsable se encargará del apoyo en la aplicación de los registros necesarios que permitan tener evidencia de los procesos a ejecutarse para la implementación del plan.

Existirán responsables de las siguientes áreas: sistemas, recursos humanos, seguridad física, servicios generales y de control interno.

4.4. PLANES DE REANUDACION

El plan de reanudación especifica los medios para mantener los servicios críticos en la ubicación de la crisis, permite regresar a las condiciones normales, este plan comenzará cuando se estimen los daños, usualmente en el día o después del desastre, y puede identificar la redefinición constante de las alternativas a ser ejecutadas.

El plan de reanudación estará vigente hasta que el daño deje de existir y los servicios sean reparados. Comprende los siguientes pasos:

- Establecimiento de la seguridad de las edificaciones.
- Reparaciones, reubicación y transferencia de operaciones clave y de los centros de control.
- Determinar la necesidad de construcciones adicionales que se requerirán para enfrentar la reanudación.
- Asegurar la reanudación de las operaciones y sus condiciones.
- Reanudar las operaciones normales del negocio.

4.5. PLANES DE RECUPERACION:

"Las estrategias de recuperación permiten precisar los objetivos de recuperación y prioridades que han sido basadas en el análisis de impacto del negocio. Estas además permiten establecer objetivos para el nivel de servicio que la organización requiere dispensar en el evento de una interrupción y el marco para luego reanudar las operaciones normales del negocio."[17]

Para efectuar los planes de recuperación se deberán desarrollar las siguientes estrategias:

- Analizar el impacto de los desastres seleccionados y las funciones críticas identificadas.
- Definir las alternativas para recuperar las funciones del negocio.
- Analizar los costos actuales y futuros de las soluciones a implementarse.
- Elegir las soluciones a implementarse.
- Los equipos de sistemas informáticos deberán establecer cual estrategia deberán aplicar, de ser el caso: recuperación interna, reemplazo de equipos, contratos con proveedores, hot site, cold site.
- Se deberán desarrollar las medidas a implementar en cada una de las etapas de: identificación del desastre, declaración del desastre, durante el desastre, recuperación del procesamiento para volver a la situación normal.
- Suscribir los contratos con los seguros de ser el caso.
- Implementar los mecanismos tecnológicos necesarios: generación de back up alternativos, implementación de enlaces paralelos, configuración de equipos.

---

[17] José Israel Castro, *Administración de la Continuidad del Negocio*, Conferencia Alemana de Cooperativas, San José, Costa Rica, 2007, p. 12.

- Asignar las responsabilidades a cada una de las personas involucradas en el plan, de acuerdo a las distintas etapas del desastre y en el mantenimiento del plan a lo largo del tiempo.
- Desarrollar los procedimientos funcionales y técnicos:
    - **Procedimientos funcionales:** la ejecución de las tareas para el personal de cada unidad, para todas las operaciones de los equipos por parte del personal especializado.
    - **Procedimientos técnicos:** para la instalación y configuración de la tecnología involucrada.

4.6 MANUAL OPERATIVO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

A continuación se establecen las reglas principales y básicas necesarias para poner en práctica el plan de continuidad del negocio:

- El plan de continuidad del negocio entrará en vigencia a partir de la aprobación de las autoridades y será responsabilidad de todos los empleados en sus diferentes funciones.
- En el caso de presentarse riesgos que atenten el normal desempeño de las actividades, se efectuarán los planes programados en conformidad al tipo de riesgo dado.
- Se conformarán los equipos de trabajo establecidos y se coordinará su inmediata participación hasta la solución definitiva y eliminación del riesgo.
- Se establecerá un proceso de control permanente hasta que la situación regrese a su normalidad, debiendo emitir informes programados sobre el avance de la situación.
- En el caso de ser necesario y dependiendo del riesgo presentado, se establecerán comunicaciones oficiales para notificación oficial del estado y su situación

- Una vez superado el riesgo se evaluarán los efectos ocurridos, los costos y se evaluarán la validez de las medidas desarrolladas a fin de disponer de la suficiente retroalimentación para mejorar el plan.
- El plan de continuidad del negocio será el documento que guíe los pasos a adoptarse en caso de enfrentar eventos que puedan ocasionar la suspensión de actividades.

4.6.1 Activación del plan

Se deberá establecer un protocolo de notificación oficial ante la ocurrencia de un desastre, además se contará con el nombre de la persona responsable para la activación de dicho protocolo.

Una vez efectuada la notificación, el responsable llamará al personal apropiado para realizar las actividades de soporte y recuperación.

a) Notificación inicial

Los procedimientos de activación del plan serán realizados después de que los planes iniciales de evacuación y respuesta de emergencias han sido implantados. Estos procedimientos de activación del plan documentan la evaluación inicial, las decisiones y las actividades de activación de equipo que serán realizadas. Se deberá proveer la coordinación y comunicación centralizada de todas las respuestas al incidente. Específicamente, estos procedimientos incluyen la activación del personal de soporte apropiado, asistencia en el desarrollo de las recomendaciones de recuperación y en la activación de los equipos de recuperación tanto de los procesos de negocio como de los de tecnología.

b) Primera notificación de alerta

La notificación de un evento contingente podría provenir de fuentes diversas, dependiendo de la naturaleza y momento de la emergencia. No obstante, la respuesta inicial a la notificación estará dictada por los procedimientos de gestión de crisis de la organización y las prácticas estándares de operación.

c) Verificación del desastre

Para la verificación del desastre se deberán seguir los siguientes pasos:

1. Si el acceso a las áreas de trabajo está disponible, se realizará una inspección para evaluar el daño de los siguientes aspectos:

1.1. Equipo electrónico (Estado: destruido, fácil de recuperar, disponibilidad de uso). Registros vitales: copias de archivos, manuales, documentación, etc. y datos en otros medios (computadoras personales, microfilm, etc.).

1.2. Equipo de oficina, trabajo en proceso, misceláneos. Analizar el estado de operación en el momento del desastre e identifique la pérdida de datos críticos. Evalúe el impacto en las operaciones si los datos deben ser restaurados desde respaldos.

2. Obtenga una evaluación de daños en relación con lo siguiente:

2.1. Tiempos de recuperación del equipo electrónico (computadoras personales, terminales y equipo de comunicaciones)

2.2. Instalaciones físicas (condiciones ambientales, integridad de la estructura física, etc.)

3. Después de la inspección, el líder del equipo de seguridad física y debe reportarse al Comité Directivo de Continuidad y Contingencia para participar en una reunión de evaluación.

d) Activación del equipo de recuperación

En cuanto el equipo responsable de la recuperación comunicará la decisión de activar el plan, el Presidente debe notificar a todos los miembros del equipo.

1. Determinar cuáles miembros del equipo deben ser requeridos para realizar los procedimientos siguientes:

1.1. Cumplir con los objetivos de recuperación

1.2. Asistir en los esfuerzos de salvamento

1.3. Asignación temporal para soportar otros departamentos

2. Elaborar una lista del personal que no es requerido en las actividades iniciales de la recuperación.

3. Obtener un lugar para hacer una reunión informativa y preparar el equipo de recuperación.

4. Contactar a todos los miembros de equipo y proveer la información siguiente:

4.1. Identificar la ubicación designada para la reunión.

4.2. Identificar los requerimientos de tiempo para preparar a los miembros de equipo.

e) Sitio alterno de respaldo de datos

En el momento de la contingencia, el responsable de la recuperación de la información deberá determinar el sitio idóneo para la ubicación de los medios de respaldo de los datos del negocio, sea una localidad en el sitio (en el centro de datos) en caso que ella no se haya visto afectada, o bien una localidad fuera del sitio.

f) Escalamiento de notificaciones

i. Basado en la severidad de la situación, se deberá determinar lo siguiente:

i.1 El evento ha sido manejado apropiadamente y no se requieren notificaciones adicionales. Terminar situación de emergencia.

i.2 Las circunstancias del evento justifican notificaciones adicionales basados en lo siguiente:

i.2.1 El evento involucra daños a la propiedad y / o personas.

i.2.2 El evento involucra una interrupción potencial del negocio que excederá las horas de un día normal de trabajo.

ii. Suministrar una breve descripción del incidente a los siguientes funcionarios:

ii.1. Coordinador del Comité Directivo del Plan de Continuidad y Contingencia

ii.2. Responsable del equipo de Seguridad Física y Servicios Generales.

ii.3. Responsable del equipo de Sistemas.

iii. Basándose en las circunstancias del evento se determinarán las acciones de respuesta inicial y el Coordinador del Comité Directivo del Plan de Continuidad y Contingencia dirigirá las siguientes actividades:

iii.1. Si daños a personal han ocurrido, notifique a Recursos Humanos para que dirija los asuntos de notificación a los familiares y establezca las prioridades de la organización durante la crisis.

iii.2. Si el acceso al edificio está permitido, inicie una inspección para evaluar los daños.

g) Evaluación de daños

Los líderes de los equipos conformados conducirán una inspección en el sitio, con el objetivo de determinar la extensión del daño en las áreas afectadas. Representantes de las áreas afectadas, de seguridad y de tecnología de información deben estar presentes para determinar las condiciones del sitio, y de los equipos de cómputo.

i. En caso de que el edificio haya sido afectado por el evento contingente:

i.1 En caso necesario, debe obtenerse aprobación de las autoridades presentes (bomberos, policía, etc.) y enviar personal a las áreas afectadas del edificio.

i.2 Determinar el equipo de emergencia que se requiere y adquirir los materiales necesarios para los miembros del equipo, basándose en las circunstancias de incidente.

Se deberá considerar, entre otros, los equipos siguientes:

 Cascos y ropa de seguridad

 Linternas

 Cámara de video / fotografía instantánea o digital

 Bloques de notas y lápices

 Radios (Walkie-talkies)

Cualquier otro que se considere necesario.

ii. El Coordinador del Comité Directivo de Continuidad y Contingencia deberá dar una charla resumida, previa a la inspección, al personal de la compañía que visitará las áreas afectadas.

ii.1 Deberá discutir la información disponible, tal como la causa, condiciones ambientales, tiempos, consideraciones especiales, etc.

ii.2 Hacer que el personal revise los procedimientos de seguridad.

iii. El Coordinador del Comité Directivo de Continuidad y Contingencia deberá asignar objetivos de inspección a cada miembro del equipo de manera que se evalúen cuidadosamente los aspectos siguientes:

- Comunicaciones

- Sistemas

- Equipo de Cómputo

- Edificio (accesos y áreas de trabajo)

- Medios de almacenamiento

iv. El Coordinador del Comité Directivo de Continuidad y Contingencia deberá viajar al sitio del daño y evaluar la magnitud del mismo. Entre otros, considerará el área y su contenido:

- Estructura (interna y externa)
- Accesibilidad dentro del edificio
- Estado de las comunicaciones
- Estado del cableado y conexiones de la red
- Estado del servicio eléctrico

v. En caso necesario, se deberá trabajar con el contratista para elaborar un estimado de la reconstrucción de las áreas dañadas.

Basándose en los resultados de la evaluación de daños, el Comité Directivo de Continuidad y Contingencia determinará si las circunstancias del incidente justifican la activación y la notificación a la jefatura respectiva. Adicionalmente, basados en esas mismas circunstancias, se debe determinar la ubicación más recomendable para el establecimiento del centro de operaciones, considerando los siguientes pasos:

i.1. Coordinar la recuperación y entrega del material almacenado fuera de sitio asignado.

i.2. Verificar que haya suficientes líneas telefónicas y teléfonos en operación.

i.3. Coordinar la entrega del equipo de cómputo requerido.

i.4. Colocar bitácoras para todo el personal que entra o sale del área asignado. Eso ayuda a documentar el uso del lugar y controlar al personal.

ii.1. Utilizar diagramas, establecer y mantener los siguientes cuadros de estado:

a) Mensajes generales
b) Ubicación del personal
c) Sesiones informativas

ii.2 En cuanto el área asignada para desarrollar el plan de continuidad esté operando, el

Coordinador del Plan será el responsable por su operación continua.

Notificación a los miembros del Comité Directivo de Continuidad y Contingencia.

Si se considera conveniente, todos los miembros del los equipos de continuidad serán contactados para que se reporten a una sesión informativa en el área asignada.

i. El Coordinador deberá suministrar la siguiente información:

i.1 Información inicial del incidente.

i.2 Ubicación, número de teléfono del área asignada.

i.3 Fecha y hora de la sesión informativa.

e) Sesión informativa

El Comité Directivo de Continuidad y Contingencia realizará una sesión informativa en el centro designado con todos los miembros del equipo invitados. Para ello utilizará como guía el siguiente procedimiento:

i. Suministrar la siguiente información, basándose en las circunstancias del evento contingente y en los resultados de la evaluación de daños.

i.1 Detalles del evento:

i.1.1. Tipo de Evento

i.1.2. Ubicación

i.1.3. Tiempo de la ocurrencia

i.1.4. Posible causa

i.2. Daños y fatalidades:

i.2.1. Número de personas muertas

i.2.2. Número de personas con heridas de gravedad

i.2.3. Estado de los heridos de gravedad

i.2.4. Posibilidad de heridos o muertos adicionales.

i.3. Edificaciones potencialmente dañadas

i.4. Acceso al edificio

i.5. Medios de Comunicación (Prensa)

i.5.1. Conocimiento del incidente por los medios (prensa)

i.5.2. Reacción de los reporteros en el sitio.

i.6. Cualquier instrucción especial o adicional que se considere conveniente y oportuna.

i.7Recomendaciones de recuperación

Una vez que se haya hecho la valoración del incidente, las actividades de respuesta y recuperación deben ser iniciadas inmediatamente y se aplicará el plan de continuidad del negocio.

5. PROPUESTA METODOLOGICA PARA LA ELABORACION DE LOS PLANES DE CONTINGENCIA

5.1 ALCANCE DEL PLAN DE CONTINGENCIA

Plan de contingencia "es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta el momento en que se produce dicho evento" [18].

La metodología define a la contingencia como la prestación ininterrumpida de los diferentes servicios que ofrece el BEV a los clientes internos y externos, superando los impases que puedan ocurrir por la presencia de situaciones que generen inestabilidad en el entorno.

La evaluación de riesgos establece los requisitos iniciales, es decir cuáles procesos críticos tendrán que ser cubiertos por el plan de contingencias, es por esto que se requerirá de un plan de contingencias para cada uno de los procesos críticos que se identifiquen.

Se tiene que estructurar una estrategia para la definición de un plan de contingencia para cada proceso crítico, esto es: recuperación total del proceso, recuperación parcial, alternativas manuales o automatizadas.

Para cada plan de contingencias es necesario estimar la posible duración de la solución alterna, junto con un estimado del tiempo que se requiere para arreglar la solución primaria.

Es necesario que se definan, para cada plan de contingencias, las condiciones que desencadenaron la activación de personas y de procesos dedicados.

El alcance del plan de contingencia aplicable al BEV se ha definido en conformidad a los siguientes elementos:

---

[18] Superintendencia de Bancos y Seguros del Ecuador, *Resolución JB-2005-834*, artículo 1, numeral 2.30.

Tipos de Incidentes comprendidos en el plan:

- Aquellos que provoquen daños físicos en las instalaciones y equipamiento tecnológico. Dentro de estos elementos se citan los siguientes: humo, fuego, fugas de agua.
- Aquellos que afecten los accesos y salidas (normales y emergencia).
- Desastres naturales. (temblores, inundaciones, etc.)
- Incidentes externos que causen impactos en los procesos del BEV, fallas de servicios básicos. (electricidad, agua, comunicación).
- Incidentes que afecten el equipamiento tecnológico, hardware y software.
- Incidentes que afecten el normal desempeño de las actividades.

El alcance del plan, no contempla los siguientes incidentes:

- Incidentes que afecten los servicios básicos en un tiempo menor a una hora.
- Incidentes de baja magnitud propios del cumplimiento normal de las actividades.

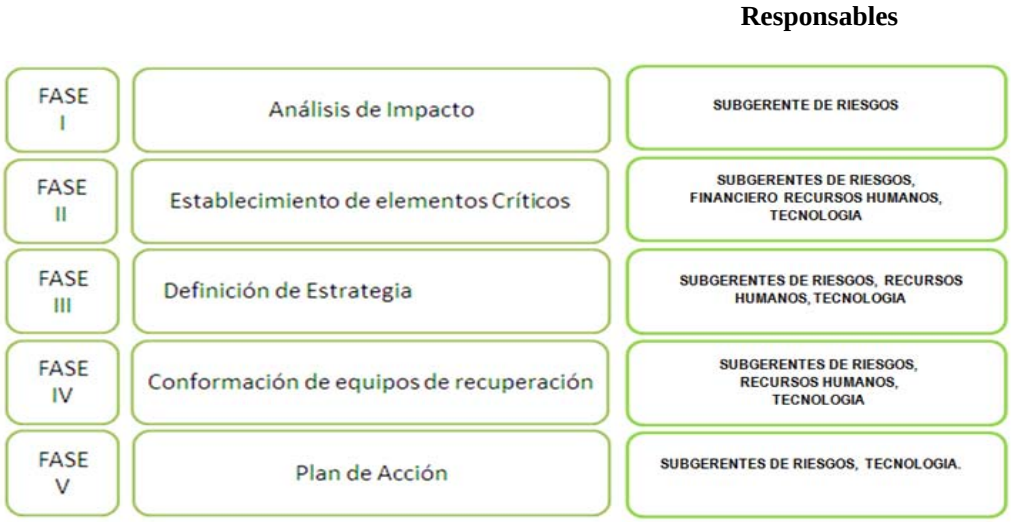
5.2 PROPUESTA METODOLÓGICA

El desarrollo de los planes de contingencia aplicables en el BEV se compone de fases que están dirigidas a establecer los mecanismos pertinentes que garanticen el funcionamiento adecuado de los diferentes procesos existentes aun cuando se presenten eventos internos o externos que afecten su desenvolvimiento, estas fases son: análisis de impacto, establecimiento de elementos críticos, definición de estrategias de contingencia, conformación de los equipos de recuperación, y el plan de acción.

Un eficiente desarrollo y aplicación de los planes de contingencia se basa en una especialización propia en las amenazas que puedan afectar los procesos en el BEV. Por esta razón, su aplicación inicia con un análisis de impacto propio que permita la definición del alcance del mismo buscando tener eficiencia y efectividad en su implementación.

GRAFICO No 16

Fases de desarrollo de la metodología para la elaboración del plan de contingencia



Elaboración: María Elena Ochoa

5.2.1 Análisis de Impacto

Uno de los principales problemas en la ejecución de un plan de contingencia es el alto costo que demanda su implementación. Por esta razón, el análisis de impacto es fundamental en el sentido de que permite tener una visión real del verdadero costo que causaría a la institución no contar con esta estructura.

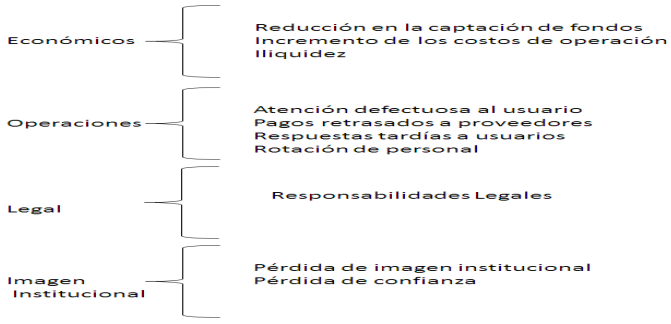
Dentro de este sentido, el proceso propuesto establece la medición del costo basado en el tiempo de recuperación, es decir por las acciones que permitan mantener la contingencia en el funcionamiento de los procesos.

De esta manera, el análisis de impacto, se establece en base a cuatro factores:

- Económicos
- Operaciones
- Legales
- Imagen Institucional

TABLA No 23

Análisis de impacto



Elaboración: María Elena Ochoa

5.2.1.1 Medición del impacto

En función de los posibles impactos a presentarse se ha establecido un mecanismo que permita su adecuada medición, esta evaluación se efectuará de manera cuantitativa y cualitativa.

a) Medición cuantitativa

La medición cuantitativa determina el impacto económico que la interrupción ha causado al BEV. La medición se realizará en escala temporal en función a los procesos afectados, utilizando para ello el siguiente formulario:

TABLA No 24

Impacto económico

	Duración de la Interrupción					
Procesos Afectados	**Horas**			**Días**		
	1	**2**	**N**	**1**	**2**	**N**
Total						

Elaboración: María Elena Ochoa

Para la medición cuantitativa se establecerán los costos incurridos durante el tiempo de recuperación. Para ello se establecen los siguientes campos de medición, los cuales fueron utilizados para la implementación del plan de continuidad:

- **RTO, Recovery time objetive.-** Se establece el tiempo que se requiere para recuperar las funciones críticas de los procesos afectados en el BEV.
- **RPO, Recovery point objetive.-** Es el tiempo establecido por la institución para respaldar su información, con el objetivo de que si sucede un evento inesperado la pérdida de datos no sea tan significativa.
- **MAO, *Maximum Aceptable Outage.-*** "Es el tiempo máximo sin servicio que una organización puede soportar y seguir siendo una compañía que cumple con sus objetivos de negocio. Normalmente este tiempo es mucho menor de lo esperado" [19].

b) Medición cualitativa

Se mide en función de la gravedad causada durante el tiempo de interrupción. Para su medición se ha establecido el siguiente formulario.

TABLA No 25

Medición cualitativa

	PROCESO					
	Gravedad					
Impacto	**Horas**			**Días**		
	1	**2**	**N**	**1**	**2**	**N**
Económico						
Operacional						
Legal						
Imagen						

Elaboración: María Elena Ochoa

La medición se realiza por cada proceso, estableciendo los siguientes parámetros de calificación:

[19]Sisteseg, *Política de Contingencia del Negocio*, p. 2

Nulo: Cuando no existe ningún impacto durante el tiempo de interrupción.

Leve: Cuando existe impacto pero no genera riesgos altos de interrupción del servicio.

- Produce interrupciones leves en el suministro de servicios con mínimo impacto en los procesos.
- Es conocido solo por algunos usuarios pero no se generaliza.
- Produce una leve falta en el cumplimiento de algún contrato.

Medio: Cuando existe impacto y genera interrupciones temporales en el servicio.

- Genera molestias en el usuario.
- Produce trastorno leve en funciones vitales.
- Pérdida de confianza, pueden existir comentarios adversos en medios locales
- Produce una falta grave en el cumplimiento de algún contrato que acarrea responsabilidades legales

Grave: Cuando el impacto genera interrupciones de gran magnitud en el servicio.

- Genera pérdidas y desgaste de imagen institucional.
- Produce interrupción inmediata de las funciones vitales.
- Pérdida de confianza en la institución
- Deja a la organización al margen de la ley

5.2.1.2 Determinación de los requisitos mínimos aceptables para la recuperación

Para el establecimiento de los procesos de recuperación en función de los impactos que puedan presentarse, es necesario definir los requisitos mínimos aceptables, situación que ayuda a la definición de los costos necesarios para su implementación.

Dentro de la definición de los requisitos mínimos aceptables se deben tomar en consideración los siguientes elementos:

- Requerimientos de personal
- Requerimientos de espacio físico

- Requerimientos de equipamiento tecnológico
- Requerimiento de bienes muebles
- Requerimientos de insumos varios

TABLA No 26

Establecimiento de los requerimientos mínimos aceptables

REQUISITOS						
DEPARTAMENTO						
	Horas			**Días**		
	1	**2**	**N**	**1**	**2**	**N**
Requerimientos de Personal						
Fijos						
Temporales						
Requerimientos de Equipos						
Fijos						
Temporales						
Requerimiento de Información						
Fijos						
Temporales						
Requerimientos de Software						
Fijos						
Temporales						

Elaboración: María Elena Ochoa

5.2.1.3 Establecimiento de estrategias

El análisis del impacto requiere de la definición de un conjunto de estrategias que permitirán aplicar eficientemente los planes de contingencias. Las estrategias se clasifican de la siguiente manera:

- Estrategias de prevención
- Estrategias de respuesta
- Estrategias de reubicación

5.2.1.3.1 Estrategias de prevención

El análisis de las amenazas más probables de ocurrencia es fundamental para establecer el posible impacto que podrían generar en los procesos del BEV.

Las estrategias de prevención, deberán garantizar tener el siguiente alcance:

- Análisis y reducción de los riesgos
- Identificación de las amenazas y vulnerabilidades
- Identificación de los riesgos potenciales
- Determinación de los niveles de riesgo
- Adopción de medidas que minimicen los impactos.

Para cada una de las estrategias de prevención desarrolladas es necesario analizar las ventajas y desventajas que puedan causar en los procesos.

5.2.1.3.2 Estrategias de respuesta

Las respuestas a los impactos ocasionados en la presencia de situaciones que alteren el funcionamiento de los procesos del BEV, deben generar respuestas inmediatas que cumplirán con las siguientes condiciones:

- Diferir la realización de las funciones de los procesos afectados
- Reubicar las operaciones del negocio durante el tiempo de recuperación
- Posponer las operaciones del negocio durante el tiempo de recuperación

La infraestructura física del BEV facilita la adopción de las medidas de respuesta ya que las áreas físicas de los diferentes departamentos pueden rediseñarse en el corto plazo dando lugar a la posibilidad del cumplimiento de las funciones que se encuentren afectadas por la presencia de riesgos.

5.2.1.3.3 Estrategias de reubicación

Dependiendo de la gravedad del impacto de los riesgos que afecten a los procesos, es necesario establecer medidas de mayor magnitud para garantizar el funcionamiento de los procesos.

La estrategia de reubicación debe enfocarse en función de la definición de instalaciones de operación alternativa.

Es necesario entender que no siempre es posible reubicar las instalaciones afectadas, para lo cual se deberá responder a las siguientes preguntas, en base a las cuales se desarrollarán los análisis posteriores:

- ¿Es posible reubicar las operaciones afectadas?
- ¿Qué procesos se pueden trasladar?
- ¿Qué procesos se pueden suprimir parcialmente sin afectar la calidad del servicio?
- ¿Cuál es la capacidad de operación en tiempo dentro de las nuevas instalaciones?
- ¿Son portables los diferentes sistemas requeridos para la operación de los procesos reubicados?

5.2.2 Establecimiento de los elementos críticos

La determinación de los requisitos mínimos aceptables permite tener una visión más clara de la criticidad de los procesos.

Se entiende de esta manera que aquellos que demanden de más cantidad de recursos para poder recuperarse generan también un mayor impacto dentro de los procesos. El análisis de la criticidad debe realizarse de una manera técnica que permita disponer de un mejor

conocimiento de los procesos del BEV. Para ello, la propuesta establece el cumplimiento del siguiente procedimiento:

- Definición de los RTO por recurso en cada proceso existente
- Establecimiento de las variables de apoyo en cada proceso
- Levantamiento de los datos
- Presentación de los informes respectivos

Para el cumplimiento del procedimiento detallado, se han diseñado formularios en función de los diferentes recursos demandados:

TABLA No 27

Requerimientos de personal

PROCESO

Requerimientos de Personal			
Descripción del Cargo	**RTO**	**Persona Propuesta**	**Suplente**

Elaboración: María Elena Ochoa

TABLA No 28

Requerimientos de espacio físico

PROCESO _____

Requerimientos de Espacio Físico					
Tipo de Puesto	**RTO**	**M^2**	**Necesidades de Comunicación**	**Conexión LAN - WAN**	**Otros Recursos**

Elaboración: María Elena Ochoa

TABLA No 29

Requerimientos de equipamiento tecnológico

PROCESO _____

Requerimientos de Equipamiento Tecnológico					
Descripción del Equipamiento	**RTO**	**Marca**	**Modelo**	**Versión (Software)**	**Servicios**

Elaboración: María Elena Ochoa

TABLA No 30

Requerimientos de bienes muebles

PROCESO _____

Requerimientos de Bienes Muebles				
Descripción del Equipamiento	**RTO**	**Modelo**	**Características**	**Observaciones**

Elaboración: María Elena Ochoa

TABLA No 31

Requerimientos de insumos varios

PROCESO _____

Requerimientos de Insumos Varios				
Descripción del Equipamiento	**RTO**	**Modelo**	**Cantidad**	**Ciclo de Reposición**

Elaboración: María Elena Ochoa

5.2.3 Definición de estrategias de contingencia

Los principales objetivos que se cumplirán si se cuenta con un adecuado desarrollo de estrategias de contingencia son: el llevar a cabo procedimientos internos de recuperación para las unidades del negocio entre el momento de ocurrencia del desastre y el momento en que el negocio esté listo para operar, el contar con localidades alternas a donde ocurrió el desastre, contar con respaldos de registros vitales en oficinas externas, reducir la confusión y el caos, permitir que el BEV pueda responder a una emergencia, planificar la recuperación y reanudación de operaciones, proteger al recurso humano como elemento esencial de la organización, establecer los recursos necesarios durante y después del desastre.

El desarrollo de las estrategias que se ejecuten para la aplicación de los planes de contingencia deberá cumplir con las siguientes premisas:

- Ser consecuentes con los planes estratégicos, los objetivos y prioridades del BEV.
- Velar porque los procesos del negocio puedan restablecerse dentro de los plazos requeridos, es decir de acuerdo a lo establecido en el análisis del impacto del negocio como el tiempo de recuperación objetivo.
- Considerar la recuperación de tecnología por cada área funcional, de acuerdo a las necesidades de: servidores, sistemas operativos y de bases de datos, accesos a la red, la capacidad global de procesamiento, los sistemas de conexión y telecomunicaciones.
- Contemplar detalladamente los procedimientos de: comunicación de crisis, respuesta de emergencia y de activación del plan.
- Las acciones a emprender una vez ocurrido el incidente respecto a: la gestión de relaciones públicas y vínculos a establecerse con autoridades nacionales pertinentes, tales como policía, bomberos, etc.
- Las acciones a emprender para el traslado de actividades esenciales de la institución a ubicaciones alternas.
- Definir alternativas de recuperación.

- Considerar los costos actuales y futuros de las soluciones a ser implementadas.
- Las estrategias para preservar la información vital de las personas de la organización deberán considerar las siguientes actividades: documentar cómo se realizan los procesos críticos, capacitar de forma multifuncional a los empleados, segregar competencias clave y planificar la sucesión del personal.
- Las estrategias deben ser detalladas y adaptables.
- Considerar el presupuesto aprobado para la implementación de los planes de contingencia.
- Considerar el apoyo de la Alta Gerencia del BEV.
- Ser probado periódicamente.
- Los controles deberán ser analizados para ser implementados en: la identificación del desastre, la declaración del desastre, las actividades a desarrollar durante el desastre y la recuperación de los procesos hasta volver a la situación normal del negocio.

La estrategia de contingencia propuesta para el BEV comprende el establecimiento de varios servicios necesarios para la adecuada funcionalidad de los procesos afectados.

Adicionalmente los responsables de la información, deberán valorar que tipo de estrategia a seguir, estas podrían ser: el centro de control frío, centro espejo, centro móvil.

Es importante que este proceso sea adecuadamente planificado para lo cual se establece el siguiente formulario:

TABLA No 32

Planificación de respaldos

Procedimiento de Backup				
Aplicación	**Fichero**	**Día**	**Periocidad**	**Versiones a conservar**

Elaboración: María Elena Ochoa

Otra alternativa es la existencia del centro de almacenamiento externo, con el fin de garantizar la existencia de la información es necesario disponer de los datos en almacenamientos externos, entendidos estos que se encuentran fuera de las instalaciones del BEV.

El avance tecnológico facilita el almacenamiento externo principalmente en *hostings* que se encuentran en servidores dedicados, que guardan la seguridad respectiva.

El proceso de *backup* planificado deberá considerar esta actividad, misma que debe permitir tener las garantías necesarias para evitar pérdidas de información.

5.2.4 Conformación de los equipos de recuperación

El Comité Directivo de Continuidad y Contingencias establecerá un lugar apropiado en donde llevará a cabo sus reuniones, que cuente con adecuados sistemas de comunicación y logística, en este sitio se evaluarán las condiciones existentes después de sucedido el incidente y se determinarán las estrategias a aplicar para mantener operativos a los procesos afectados.

Adicionalmente el Comité conformará equipos compuestos por personal calificado, que actúe en forma eficiente e inmediata frente a las amenazas presentadas.

La conformación de los equipos de recuperación para los planes de contingencia dependerá del Comité Directivo de Continuidad y Contingencia y se clasificará de la siguiente manera:

- Equipo de gestión de incidentes
- Equipo de operaciones informáticas
- Equipo de administración
- Equipo de atención a usuarios
- Equipo de inmuebles
- Equipo de servicios generales

a) Equipo de gestión de incidentes

Estará conformado por los jefes de todos los departamentos del BEV. Sus funciones son:

- Planificar la realización de actividades que mantengan en garantía la contingencia de las operaciones
- Realizar los informes del estado de la situación en los diferentes procesos
- Evaluar los daños existentes en la presencia de las amenazas en los procesos

b) Equipo de operaciones informáticas

Su principal responsabilidad es garantizar la existencia de datos e información en todos los procesos aun cuando estos estén afectados.

Para ello, cumplirán con las siguientes funciones:

- Instalación de las soluciones planificadas
- Cumplir la planificación de backup
- Realización de pruebas de funcionamiento
- Recuperación del sistema operativo
- Comprobar la veracidad de los datos existentes

c) Equipo de administración

Su función principal es la de dotar del equipamiento necesario y las instalaciones requeridas para el funcionamiento de los procesos afectados. Cumplirá con las siguientes responsabilidades:

- Administrar los fondos existentes para la aplicación del plan de recuperación de bienes inmuebles
- Coordinar la seguridad del edificio

- Coordinar los contratos de seguros de los bienes
- Identificar los problemas existentes con el talento humano
- Establecer relaciones con medios de comunicación para la difusión de mensajes y noticias pertinentes.

d) Equipo de atención a usuarios

Su función principal es la de mantener informado a todo el personal de los cambios o acciones necesarias a cumplir en función de las amenazas o riesgos presentados en los diferentes procesos.

Representará la voz oficial de todas las medidas implementadas a fin de evitar rumores que generen inestabilidad en su aplicación y recuperación.

e) Equipo de inmuebles

Responsable del acondicionamiento de las instalaciones a utilizar para la contingencia en los procesos afectados. Supervisará que las instalaciones reúnan todas las condiciones necesarias para poder cumplir eficientemente con las funciones a cumplir.

Verificará con el equipo de administración, que las instalaciones se encuentren debidamente equipadas a fin de evitar problemas en su funcionamiento.

f) Equipo de servicios generales

Brindará soporte en cualquier servicio adicional que se necesite en el proceso de recuperación.

5.2.5 Plan de acción

El plan de acción comprende la puesta en marcha de las acciones planificadas que permitan recuperar en forma inmediata los daños provocados por la presencia de amenazas en

los diferentes procesos. De igual manera establece las acciones preventivas que eviten la presencia de las amenazas. A continuación el detalle de estas acciones:

5.2.5.1 Acciones de emergencia del plan de acción

- Establecer las medidas necesarias en el caso de existir heridos o víctimas mortales por la presencia de las amenazas.
- Coordinar la preparación de la información pública a socializar a la sociedad.
- Programar las acciones de los equipos de recuperación para garantizar su funcionamiento las 24 horas.
- Designar los medios de comunicación temporales a utilizar.
- Coordinación de la ubicación del personal en los lugares asignados.
- Mantener informado al personal sobre la evolución de la situación.

5.2.5.2 Preparación del informe

Todo proceso de recuperación emitirá informes sobre las acciones desarrolladas, debiendo abarcar la siguiente estructura.

a) Estado de las actividades de respuesta de emergencia:

- Evacuación del edificio
- Respuesta de las autoridades

b) Descripción del incidente:

- Localización del incidente
- Hora del suceso
- Cobertura del suceso

c) Informe de heridos o víctimas:

- Nombre de las víctimas mortales
- Nombre y estado de los heridos
- Lugar donde han sido trasladados

- Víctimas potenciales adicionales

d) Áreas afectadas:

- Departamentos involucrados
- Estado actual
- Impacto en las operaciones del negocio

f) Estado del plan de acción:

- Situación de las comunicaciones
- Planes desarrollados
- Resultados obtenidos

El plan de acción se compone de tres tipos de procedimientos que se detallan a continuación:

5.2.5.3 Procedimientos de emergencia

Incluyen las acciones inmediatas que se deben cumplir para proteger la integridad del funcionamiento de los procesos.

Su aplicación se ejecuta en función de alertas en base a una escala de importancia.

- Primera Alerta: aviso preliminar
- Segunda Alerta: preparación de los equipos
- Tercera Alerta: aplicación de los planes de contingencia.

5.2.5.4 Procedimientos de respuesta

Incluyen la aplicación de actividades complementarias necesarias para minimizar los impactos negativos posibles a presentarse y restablecer el normal funcionamiento del proceso.

5.2.5.5 Procedimientos de recuperación

Incluyen los procedimientos que permiten mantener los datos y la información necesaria para el funcionamiento de los procesos.

La aplicación del plan de acción se conformará en base al cumplimiento de los siguientes elementos:

- Determinar quien ejecutará las acciones en cada uno de los procedimientos
- Determinar los tiempos de aplicación de las acciones planificadas
- Definir el proceso de comunicación para los diferentes integrantes del equipo
- Establecer los procedimientos de valoración de los daños
- Establecer los formularios para la presentación de los informes requeridos

La preparación de los procedimientos de recuperación debe también disponer de un área física adecuada para la coordinación de las actividades necesarias.

Se deberán ejecutar los siguientes pasos:

a) Procedimientos de recuperación del sistema operativo

Necesarios para garantizar el funcionamiento de los diferentes sistemas requeridos por los procesos.

b) Procedimientos de recuperación de aplicaciones

Se recuperarán todas las aplicaciones necesarias para el funcionamiento de los procesos en los diferentes departamentos.

c) Procedimientos de recuperación de datos

Necesarios para garantizar la existencia de los datos para el cumplimiento de las respectivas operaciones.

d) Plan de vuelta a la normalidad

El establecimiento de las acciones que permitan volver a la normalidad en el menor tiempo posible, demandan de las siguientes actividades:

- Desarrollar las sesiones necesarias para definir las estrategias que permitan volver a la normalidad de las funciones.
- Revisar cada proceso de recuperación implementado.
- Verificar cualquier recomendación que mejore los procedimientos implementados.
- Establecer los procedimientos modificados si existieran.

5.2.6 Pruebas y actualización

Los objetivos para la ejecución de pruebas de los planes de contingencia son: asegurar que el plan es operacional, garantizar que está actualizado, que es eficaz y que todos los miembros del equipo conocen y son parte de este plan.

Las pruebas que se ejecutarán serán dinámicas, es decir permitirán establecer si el equipo que implementará los planes de contingencia cumple con los requerimientos operacionales necesarios, adicionalmente se comprobará que las acciones a ser desarrolladas son efectuadas de acuerdo a la realidad cambiante del BEV.

De acuerdo a los escenarios establecidos el equipo encargado de efectuar las pruebas, determinará los tipos de pruebas a ser ejecutadas, estas pueden ser: programadas, de escritorio, de simulación, de discusión, funcional, de recuperación técnica, de sitio alterno, de simulacro, integral o a gran escala, por sorpresa.

Las pruebas y actualizaciones requeridas deberán cumplirse en función de las siguientes actividades:

- Revisiones periódicas para verificar el funcionamiento
- Ejercicios de entrenamiento

- Pruebas técnicas

5.2.6.1 Mantenimiento del plan

Los planes de contingencia deben mantenerse mediante revisiones y actualizaciones periódicas para garantizar su eficacia permanente ante cambios de: personal, direcciones, números telefónicos, estrategia de negocios, ubicación, instalaciones y recursos.

Finalmente, se deben establecer medidas que permitan al plan funcionar adecuadamente. Para ello se establecerán las siguientes acciones:

- Garantizar que los equipos actualicen el plan de contingencia en función de los cambios existentes.
- Revisar si los recursos existentes son necesarios en función de los cambios en el plan de contingencia.
- Revisar periódicamente las estrategias de implementación
- Mantener actualizaciones de la información, datos y sistemas existentes en cada uno de los procesos.
- Establecer los cambios de personal que sean necesarios en función de evaluaciones de desempeño.

El plan de contingencia establecido representa un mecanismo que garantiza al BEV la contingencia en el desempeño de sus funciones para evitar interrupciones que afecten a nivel económico, legal, operativo y de imagen a la institución.

Como se puede apreciar, demanda de una serie de recursos pero que deben estar debidamente justificados en función de los altos costos para este tipo de medidas.

El plan presentado ha dado importancia al talento humano, conformando una estructura debidamente organizada cuya asignación de funciones se encuentran encaminadas a brindar todas las facilidades para su adecuada implementación.

De igual manera, se han establecido medidas para proteger la información, misma que se respaldará tanto interna como externamente, a fin de permitir siempre el funcionamiento de los procesos.

5.2.7 Evaluación de la infraestructura existente

El Banco Ecuatoriano de la Vivienda deberá elaborar la presentación gráfica en planos de la localización, de los medios de protección y vías de evacuación existentes en toda la edificación.

Estos planos, realizados en un formato y escala adecuada, contendrán como mínimo la siguiente información:

- Vías de evacuaciones principales y alternativas.
- Medios de detección y alarma.
- Sistema de extinción fija y portátil, manuales y automáticos.
- Señalización y alumbrado de emergencia.
- Existencia de materiales inflamables y otros de especial peligrosidad.
- Ocupación por zonas.

5.2.7.1 Factores a tener en cuenta en la evaluación de la infraestructura

- **Densidad de ocupación de la edificación.-** Dificulta el movimiento físico y la correcta percepción de las señales existentes, modificando el comportamiento de los ocupantes. A su vez, condiciona el método para alertar a los ocupantes en caso de emergencia y agudiza el problema.
- **Características de los ocupantes.-** En general toda edificación, instalación o recinto es ocupada por personas de distintas características como son: edad, movilidad, percepción, conocimiento, disciplina, entre otras.
- **Existencia de personas ajenas.-** Aquellas edificaciones, instalaciones o recintos ocupados en su totalidad por personas que no los usan con frecuencia, y por ello no están familiarizados con los mismos. Ello dificulta la localización de salidas, de vías

que conducen a ellas o de cualquier otra instalación de seguridad que se encuentre en dichos locales.

- **Condiciones de Iluminación.-** Da lugar a dificultades en la percepción e identificación de señales, accesos a vías de escape, etc., y a su vez incrementa el riesgo de caídas, golpes o empujones.

La existencia de alguno de estos factores o la conjunción de todos ellos junto a otros que puedan existir, previsiblemente darían lugar a consecuencias catastróficas ante la aparición de una situación de emergencia, si previamente no se ha previsto tal evento y se han tomado medidas para su control.

5.2.8 Priorización de los sistemas

El BEV es una institución que abarca un conjunto de procesos y actividades considerables, por lo que la metodología sugiere su aplicación en base a un sistema de priorización que busca concentrarse inicialmente en las actividades de mayor nivel de criticidad, es decir aquellas que por su condición y desarrollo son las más vulnerables a sufrir la ocurrencia de riesgos.

Una vez priorizadas las áreas de gestión, el proceso deberá iniciar con la aplicación de la metodología. Es importante señalar que una vez cubiertas las áreas críticas, se deberá cumplir con todos los procesos ya que la falta de alguno podría comprometer seriamente la eficiencia de la metodología.

A continuación el detalle de los aplicativos y los procesos del negocio que soportan la infraestructura tecnológica que posee el BEV, adicionalmente se indica la prioridad de cada módulo:

TABLA No 33

Detalle de aplicativos y procesos del negocio

(Ver siguiente página)

No	Producto	Ambito de Acción	Módulos que se relaciona Procesos Críticos	Prioridad
	Programas y Aplicaciones			
1	SRC	Subgerencia de Negocios - área de recuperación de cartera	Producto de Cartera	Alta
2	Caja Cartera BEV-MB	Subgerencia de Operaciones	Producto de Cartera	Alta
3	Cartera Castigada	Subgerencia de Operaciones	Producto de Cartera	Alta
4	Caja de Servicios	Subgerencia de Operaciones	Producto de Cartera	Alta
5	Banco de Fomento	Subgerencia de Operaciones	Producto de Cartera	Alta
6	Fondos en Garantía	Subgerencia de Operaciones	Fondeo/Fondos en Garantía	Alta
7	SFI	Subgerencia Financiera y demás subgerencias		Alta
8	Cajas Externas	Subgerencia de Operaciones	Producto de Cartera	Alta
9	Proceso de Depositos receptados a traves del Banco de Fomento	Subgerencia de Operaciones	Producto de Cartera	Media
10	EVOLUTION	Subgerencia de Recursos Humanos		Baja
11	Proveeduría	Subgerencia Administrativa		Baja
12	Mantenimiento Mecánico	Subgerencia Administrativa		Baja
13	Activos Fijos	Subgerencia Administrativa		Media
14	Central de Riesgos	Subgerencia de Riesgos		Media
15	Presupuesto	Subgerencia Financiera		Alta
16	Registro Contable y Control de Pagos	Subgerencia Administrativa		Alta
17	Módulo de Riesgos	Subgerencia de Riesgos		Alta
18	Sistema de Compra de Cartera	Subgerencia de Negocios		Alta
19	Sistema de Fideicomisos	Subgerencia de Negocios	Fideicomisos inmobiliarios	Alta
20	Sistema de Inversiones	Subgerencia Financiera		Alta
21	Ahorros	Subgerencia de Operaciones	Fondeo/ Ahorros	Alta
22	Banca de Segundo Piso	Subgerencia de Negocios	Producto de Cartera	Media
23	Banca Virtual	Subgerencia de Operaciones		Media Alta
24	Apertura de Cuentas por la WEB	Subgerencia de Operaciones		Media Alta
25	Depósitos a las cuentas de ahorros en la WEB	Subgerencia de Operaciones		Media Alta
26	Autorizaciones por la WEB	Tecnología		Media Alta
27	Seguridades	Tecnología		Alta
28	Bienes Inmuebles	Subgerencia Administrativa		Baja

Elaboración: María Elena Ochoa **Fuente: BEV**

La organización deberá establecer la forma en que implementará el centro alternativo para responder a la contingencia presentada.

5.2.9 Estructura del plan de contingencia

Se deberán desarrollar procedimientos funcionales, dentro de los cuales se observarán la ejecución de las tareas del personal de cada sector y para la operación de los equipos por parte del personal especializado.

Adicionalmente el detalle de los procedimientos técnicos servirá para establecer las actividades de instalación y configuración de la tecnología involucrada.

El Manual del plan de contingencia deberá contener:

- Nota de introducción: en ella se establecerán los objetivos principales para efectuar los planes de contingencia.

- Política general y alcance: se establecerán los lineamientos en que se deberá basar la estructuración de los planes de contingencia y su ámbito de ejecución.
- El Gobierno: se detallarán la estructura y las funciones del Comité Directivo de Continuidad y Contingencia y de los responsables de implementar los planes de contingencia.
- La estructura de contingencia: las fases necesarias para llevar a cabo los planes de contingencia.
- Los roles y responsabilidades de los funcionarios encargados de los equipos de contingencia.
- Normas, de acuerdo a la norma ISO 27001, se deberá establecer: el tratamiento de la información, los responsables de seguridad, la administración de usuarios y permisos, licencias legales, copias de respaldo, correo electrónico y uso de internet, ambientes de procesamiento, comunicaciones, antivirus, protección física, auditoria automática, contingencia del procesamiento.
- Línea de sucesión: como se implantará la alerta y quien será el encargado de tomar el mando en caso de requerir se declare una contingencia.
- Cadena de llamadas: se deberá mantener un listado con los teléfonos actualizados del personal que conforma los equipos de contingencia y los responsables en comunicar a otros funcionarios.
- Procedimientos generales: se mantendrá un detalle de todos los procesos normales del negocio, cuando no se ha trabajado en contingencia.
- Procedimientos alternos para trabajar bajo contingencias: se mantendrá un detalle de los procesos que se ejecutarían al tener una contingencia, y los dispositivos a ser utilizados para su desarrollo.

- Procedimientos de mantenimiento: en este se detallan los procesos que son necesarios para mantener actualizados los planes de contingencia.
- Estrategias del plan de contingencia: se deberá definir si es documento abierto o clasificado, la confidencialidad y seguridad de la empresa.
- El documento deberá contener un anexo, en donde se describa: el glosario de términos, en este se detallan los conceptos que han sido utilizados en la elaboración de los planes de contingencia y su significado, con el fin de que todas las personas involucradas tengan el mismo conocimiento sobre las palabras empleadas.
- En otro anexo se deberán citar: Las sanciones por incumplimientos, se deberán detallar las sanciones por la inobservancia de las políticas de contingencia.

Los planes de contingencia deben ser probados, superar las pruebas que confirmen su efectividad, ser divulgados y conocidos por todos los responsables de su ejecución en sus diferentes etapas. Adicionalmente los planes de contingencia deben ser objeto de revisión y actualización por lo menos cada año.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

Una vez terminada la realización del estudio, se presentan las siguientes conclusiones:

1. El Banco Ecuatoriano de la Vivienda al ser una institución financiera pública debe mantener vigentes sus políticas de continuidad del negocio, con el fin de asegurar la supervivencia de la entidad en caso de que esta se vea sometida a una interrupción en su funcionamiento.

2. La metodología propuesta para la implementación del plan de continuidad del negocio del BEV se desarrolló considerando las mejores prácticas de riesgo operativo; las principales normas en que se basó este estudio fueron la norma británica BS 25999 y la entregada por el Comité de Basilea, pues en ellas se obtuvo una guía adecuada para la formulación de las fases de la implementación de los planes de continuidad de los negocios. La principal ventaja de estas prácticas es que se enfoca en la cadena de valor de la empresa, en sus procesos críticos y en la evaluación de los impactos del negocio. La principal desventaja es que requiere de una cantidad considerable de recursos tanto económicos como humanos.

3. El gobierno corporativo del BEV debe reconocer y considerar la importancia de contar con planes de contingencia y de continuidad del negocio, con el fin de comprometer la entrega de los recursos necesarios para la implementación de estos planes en la institución, este apoyo será clave para que el proyecto propuesto sea exitoso.

4. La gestión de la continuidad y contingencia del negocio es un proceso continuo que permite identificar posibles impactos que amenazan al normal desenvolvimiento de las operaciones y provee de lineamientos para que las instituciones puedan responder de forma efectiva ante cualquier evento, con el fin de salvaguardar los intereses de sus accionistas, su reputación y sus actividades de creación de valor.

5. El establecimiento de los procesos críticos del banco constituye el punto de partida sobre el cual se desarrollará la implementación de la metodología propuesta, en todos estos se efectuará la evaluación de los riesgos, los análisis de impacto del negocio, el periodo de recuperación de los elementos críticos y los tiempos máximos de interrupción, que serán considerados para el desarrollo de los planes de continuidad y contingencia.

6. Las metodologías propuestas pretenden resaltar la importancia de la implementación de los planes de contingencia y continuidad en el negocio, ya que éstos constituyen un factor fundamental para la generación de confianza por parte de los clientes, los empleados, los proveedores y la comunidad en general, que tienen relación con el Banco Ecuatoriano de la Vivienda.

7. La efectividad de la metodología para el desarrollo de los planes de continuidad y contingencia en el BEV, dependerá de la comprensión y las acciones que puedan efectuar los responsables de su implementación, ya que los planes deben adaptarse a la realidad de la institución y al ambiente en que se desarrolla.

8. Para que la metodología propuesta tenga efectividad, los responsables deberán cerciorarse que el BEV posee los recursos humanos, logísticos, económicos y tecnológicos para el desarrollo de los planes de continuidad y contingencia. Personalmente pienso que el BEV debería contar con una infraestructura tecnológica de alta disponibilidad de recursos, tanto de hardware como de software, con lo que se lograría que el tiempo de operatividad sea el adecuado.

6.2 RECOMENDACIONES

Se plantean las siguientes recomendaciones en función de las conclusiones presentadas:

1. La gestión de continuidad del negocio deberá formar parte del Sistema de Administración Integral de Riesgos del BEV, por lo que es necesario se consideren aspectos relacionados con el análisis de riesgos, el impacto y probabilidad de ocurrencia de los eventos de riesgo y los controles a ser ejecutados para la continuidad del negocio.

2. Es necesario que el Directorio del BEV sea el responsable de la implementación de los planes de continuidad del negocio, por lo que deberá dictar políticas referentes a la continuidad de operaciones, además es el encargado de fomentar una cultura de riesgos institucional en donde se establezca la importancia de contar con elementos de continuidad del negocio.

3. La Gerencia del Banco Ecuatoriano de la Vivienda deberá comunicar las políticas establecidas, a través de reuniones con los encargados de cada una de las áreas involucradas en el desarrollo de los planes de contingencia y continuidad. Se deberán establecer claramente las actividades detalladas en la metodología, las responsabilidades del personal y los cronogramas de acción para ejecutar las fases propuestas.

4. El BEV deberá incluir dentro de su estructura orgánica administrativa la creación del Comité Directivo de Continuidad y Contingencia, y la definición de sus responsabilidades y alcances.

5. La entidad deberá efectuar pruebas periódicas a sus planes de contingencia y continuidad que permitan validar las acciones que se efectuarán, con el objetivo de recobrar las operaciones críticas, consideradas en los planes de continuidad del negocio.

6. Los empleados del BEV deberán conocer, gestionar y aplicar los lineamientos y estrategias de continuidad del negocio, con el fin de proteger a las personas, los bienes y la información de la entidad.

7. El Banco Ecuatoriano de la Vivienda deberá verificar que la gestión de los procesos responde a niveles óptimos y requeridos por el negocio, antes, durante y después de la ocurrencia de un evento de interrupción.

8. El Banco Ecuatoriano de la Vivienda con el fin de mantener la continuidad del negocio deberá desarrollar altos niveles de servicio tecnológico, a través de la implementación de procesos e infraestructura tecnológica eficiente y actualizada.

9. Debido a que las condiciones del entorno varían constantemente, es importante que se revisen continuamente las metodologías planteadas, con el fin de actualizarlas de acuerdo a la realidad cambiante de la institución.

10. Es un requisito indispensable que los mecanismos de seguridad informática sean los óptimos dentro de la institución con el objetivo de que estos detecten oportunamente alteraciones en las bases de datos, por lo que se recomienda establecer sistemas de seguridad con certificaciones internacionales, con el fin de reducir riesgos informáticos.

11. Se recomienda que la institución mantenga constante comunicación con los organismos encargados de proporcionar seguridad y auxilio dentro del país, como son: policía, bomberos, cruz roja, etc., con el fin de plantear programas conjuntos de contingencia; adicionalmente se deberán coordinar las relaciones públicas con la prensa nacional.

12. El contar con planes de continuidad y contingencia significará que el gobierno corporativo del BEV pueda establecer elementos que le permitan tomar decisiones respecto a sus procesos críticos y los controles que deberá implementar para mitigar, transferir o asumir los riesgos que se puedan presentar.

BIBLIOGRAFÍA

Libros y Revistas

- Amaya Amaya, Jairo, *Sistemas de Información,* Universidad Santo Tomás, ECOE Ediciones, 2005

- Baquero Herrera, Mauricio, *La Nueva propuesta del Comité de Basilea relacionada con Estándares de Supervisión Bancaria*, 2008

- Castro, José Israel, *Administración de la Continuidad del Negocio*, Conferencia Alemana de Cooperativas, San José, Costa Rica, 2007.

- Goh Moh, Heng, *Developing a Suitable Business Continuty Planning*, Estados Unidos, Mcb Up Ltd, 2008.

- Lopez, Pascual J. y González, Sebastián, *Gestión Bancaria, Los Nuevos Retos de un Entorno Global*, Editorial Mc Graw-Hill, España, 1998.

- Martínez Gaspar, Juan, *El Plan de Continuidad del Negocio, Guía Práctica para su elaboración*, ediciones Díaz Santos, Madrid, España, 2006.

- Morales Díaz, José, *La Ley Sarbanes Oxley y la Auditoría*, Ernst & Young LLP, 2004.

- Porter, Michael E, *Estrategia Competitiva*, Editorial Continental, México, 1996.

- Porter Michael E., *Ventaja Competitiva*, Editorial Continental, México, 1996

- Laviada Fernández, Ana, *La Gestión del Riesgo Operacional*, UCEIF Ediciones, 2010

- Soler Ramos, José A., Staking Kim B. y otros, *Un Enfoque Práctico Para Países Latinoamericanos, Gestión de Riesgos Financieros*, Banco Interamericano de Desarrollo, Washington, 1999.

- Sisteseg, *Política de Contingencia del Negocio*, 2008.

Leyes, Reglamentos y Normas

- BS 25999, *Código de Buenas Prácticas de la Gestión de Continuidad del Negocio.*
- Comité de Supervisión Bancaria de Basilea, *Buenas Prácticas para la Gestión y Supervisión del Riesgo Operativo*, Secretaría del Comité de Supervisión Bancaria de Basilea, 2003.
- Comité de Supervisión Bancaria de Basilea, *High-level principies for Business Continuity*, 2005
- Ley Sarbanes Oxley (SOX)
- Informe del Committee of Sponsoring Organizations - COSO ERM (Enterprise Risk Management)
- IT Gorvenance Institute, Cobit 4.0, *Objetivos de Control, Directrices Generales, Modelos de Madurez*, Norma Técnica Ecuatoriana.
- NTE INEN-ISO/IEC 27002:207009, *Tecnología de la Información-Técnicas de la Seguridad, Código de Practica para la Gestión de la Seguridad de la Información.*
- ITIL: 2007, ITIL V3 Glossary, 30 May 2007, en http://www.best-management-practice.com/gempdf/ITIL_Glossary_V3_1_24.pdf
- Superintendencia de Bancos y Seguros del Ecuador, *Ley de Instituciones del Sistema Financiero*, Quito, 2007.
- Superintendencia de Bancos y Seguros del Ecuador, *Resolución de Riesgo Operativo JB-2005-834,* 2005.
- The BCI, *Glossary of Business Continuity Management Terms*, 2009, en http://recoveryspecialties.com/glossary.html

- U.S. Securities and Exchange Comision, *SEC, Initiatives Ander New Regulatory Reform Law.*